ANALISIS DE DESEMPEÑO DE SOFTWARE DE DETECCIÓN DE VULNERABILIDADES COMO HERRAMIENTA PARA IMPLEMENTAR ESTUDIO DE SEGURIDAD COMPUTACIONAL EN REDES LOCALES.

ING. LUZ ÁNGELA BARRAGÁN ORTIZ

TESIS PARA OPTAR EL TITULO DE MAESTRIA EN INGENIERIA: AREA EN INFORMATICA Y CIENCIAS DE LA COMPUTACION

DIRECTOR

PhD. JUAN CARLOS GARCIA DIAZ

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERIAS FISICO-MECANICAS
MAESTRIA EN INFORMATICA
BUCARAMANGA
2.004

ANALISIS DE DESEMPEÑO DE SOFTWARE DE DETECCIÓN DE VULNERABILIDADES COMO HERRAMIENTA PARA IMPLEMENTAR ESTUDIO DE SEGURIDAD COMPUTACIONAL EN REDES LOCALES.

ING. LUZ ÁNGELA BARRAGÁN ORTIZ

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERIAS FISICO-MECANICAS
MAESTRIA EN INFORMATICA
BUCARAMANGA
2.004

AGRADECIMIENTOS

La autora expresa sus agradecimientos a:

JUAN CARLOS GARCIA DIAZ. Ingeniero de Sistemas, Director de la Tesis.

HECTOR GIL TRIANA. Ingeniero de Sistemas.

ALEX DELGADO. Ingeniero de Sistemas.

JUAN CARLOS MARTINEZ. Ingeniero de Sistemas.

MARTHA LUZ CRISTANCHO MORENO. Ingeniera de Petróleos.

MARIA EUGENIA ANGARITA. Secretaria de la Maestría en Informática.

GABRIEL VARGAS. Ingeniero Mecánico.

A las personas que de una u otra forma colaboraron en la realización de esta Tesis.

DEDICATORIA

A Dios consagro mi ser,

A mi Madre, Mery, ofrezco mi dedicación y esmero,

A mi Esposo, Aquileo y a mi hijo, Juan David, todo mi amor y un nuevo horizonte para los tres,

A mis Hermanos y Sobrinos mi compromiso,

A mis Familiares, CLASS y Amigos mi éxito, esta etapa de mi vida y mi sincera amistad.

Luz Angela.

TABLA DE CONTENIDO

PAGINA

TITULO: ANÁLISIS DE DESEMPEÑO DE SOFTWARE DE DETECCIÓN DE VULNERABILIDADES COMO HERRAMIENTA PARA IMPLEMENTAR ESTUDIOS DE SEGURIDAD COMPUTACIONAL EN REDES LOCALES.

AUTOR: BARRAGÁN ORTIZ, Luz Angela

PALABRAS CLAVES: Seguridad Computacional, Vulnerabilidad, Escaneo de Redes

Los productos evaluadores de vulnerabilidades, también conocidos como rastreadores de vulnerabilidad, son desarrollos que efectúan auditorías de seguridad sobre los sistemas en uso, buscando cuales son los puntos en que son vulnerables a cierto tipo de ataques.

Estos productos tienen dos enfoques para localizar e informar las vulnerabilidades a la seguridad que encuentran. El primero, llamado rastreo o escaneo pasivo, revisa la configuración del sistema, en lo que se relaciona con los permisos de los archivos, la propiedad declarada en los archivos críticos, la configuración de los paths y busca configuraciones que la experiencia ha demostrado que generan problemas de seguridad. El segundo enfoque, un escaneo o rastreo activo, recrea una serie de ataques conocidos realizados por hackers y registra los resultados de los mismos. Algunos de estos productos también desarrollan el crackeo de los archivos de contraseñas para descubrir aquellas incorrectas o débiles que podrían ser fácilmente adivinadas por los hackers. Finalmente el producto registra sus hallazgos en pantalla o en algún otra forma de informe.

Los productos evaluadores de vulnerabilidades son una parte valiosa de cualquier programa de administración de la seguridad de los sistemas en cualquier organización. Le permite a los responsables delimitar o establecer una línea de seguridad en todo el sistema. Permiten llevar a cabo auditorías periódicas de seguridad para determinar la salud del sistema en un momento preciso. Muchos proveen la capacidad de desarrollar análisis diferenciados, archivando los resultados de los rastreos, para luego compararlos con los siguientes realizados sobre los archivos e informando cuando aparece una nueva vulnerabilidad o un cambio inesperado.

El análisis de vulnerabilidades trabaja en conjunto con los antivirus, firewall y sistemas de detección de intrusos, formando así los cuatro pilares de la seguridad en redes. Además los sistemas corporativos requieren otras herramientas de gestión como las políticas de seguridad y el plan de contingencia, para mantener su seguridad informática.

TITLE: THE ANÁLISIS OF PERFOMANCE OF VULNERABILITIES DETECTION SOFTWARE AS TOOL TO IMPLEMENT STUDY OF COMPUTATIONAL NETWORK SECURITY.

AUTHOR: BARRAGÁN ORTIZ, Luz Angela

KEY WORDS: Network security, Scann Network

The tester products of vulnerabilities, are also known as scanners of vulnerability, they are developments that carry out audits of security about systems in use, looking for the points in which they are vulnerable to some kind of attacks.

These products have two approaches to search and inform the vulnerabilities to the security they find out. The first, called passive scanning, make a revision of the system configuration, in which it is related to the files permissions, the property declared in the critic files, the paths configurations and look for configurations that experience has shown that generate problems of security. The second approach, an active scanning, it reproduces series of known attacks carried out by hackers and the results of the same attacks are registered. Some of these products also develop the password files crack. In order to discover those which are wrong or weak that could be easily guessed by hackers. Finally, the discoveries are registered on a screen or in an any other way of report, by the product.

The tester products of vulnerabilities are a valuable part of any administration program of systems security in any organization . It permits the responsible ones delimit or establish a security line in all of the new systems. They permit them to carry out periodical audits of security to determine the system heath in a specific moment. Many of them provide the capacity to develop differentiated analysis, filing the results of scanning, in order to compare them later with the next ones carried out about the files and informing when a new vulnerability or an unexpected change appears.

The vulnerabilities analysis works together with the antivirus, firewall and systems of intruders detection, integrating the four main principles of nets security. Moreover, the corporative systems require another tools of work like the security policies and the contingency plan, to keep its computational security.

1. DESCRIPCIÓN GENERAL DEL PROYECTO

1.1. TITULO

Análisis de Desempeño de Software de Detección de Vulnerabilidades como Herramienta para Implementar Estudios de Seguridad Computacional en Redes Locales.

1.3. OBJETIVOS

1.2.1. OBJETIVO GENERAL

Analizar el desempeño de herramientas software de detección de vulnerabilidades, con el fin de implementar seguridad computacional en una red local.

1.2.2. OBJETIVOS ESPECIFICOS

- Elaborar una revisión bibliográfica sobre redes: fallas de seguridad, ataques más frecuentes y herramientas software de detección de vulnerabilidades.
- Diseñar y conducir las pruebas del software de detección de vulnerabilidades con el fin de evaluar su desempeño.
- Generar un reporte escrito con los resultados del análisis que sirva de referencia para implementar de seguridad en redes.

2. PLANTEAMIENTO DEL PROBLEMA

La seguridad en los sistemas de información y de cómputo se ha convertido en uno de los problemas más grandes desde la aparición, y más aun, desde la globalización de Internet. Dada la potencialidad de esta herramienta y de sus innumerables aplicaciones, cada vez más personas y empresas sienten la necesidad de conectarse a este mundo.[1]

Aunque, la Seguridad no es una función nueva de la empresa, ni una necesidad sobrevenida por el uso de Redes Telemáticas, actualmente merece mayor atención por parte de los administradores de redes Datos debido a:

- Las redes son los medios digitales más usados en todos los ámbitos de la sociedad para la transferencia de información.
- Normalmente estos medios se encuentran en redes públicas, por lo cual están expuestas a intervenciones de una u otra forma.
- El amplio desarrollo de las nuevas tecnologías informáticas, está ofreciendo un nuevo campo de acción a conductas antisociales y delictivas manifestadas en formas antes imposibles de imaginar, ofreciendo la posibilidad de cometer delitos tradicionales en formas no tradicionales.[2]

Son muchas las vulnerabilidades que puede tener en sistema de computo, si se piensa en que cualquier situación o acción que atente contra las premisas de la seguridad computacional, aprovechando alguna deficiencia, es materia de análisis.[3]

Es frecuente que cada semana la prensa especializada en los sistemas de información hablen de otro fallo de seguridad: un virus que se aprovecha de las macros que manejan las herramientas del Office de Microsoft, una vulnerabilidad en Windows o UNIX, un problema de Java, un agujero de seguridad en una de las páginas principales de Internet, un ataque contra un popular cortafuegos.[3]

Una forma común de "probar" la seguridad es realizar revisiones de seguridad. Esto es un proceso manual costoso y requiere de un tiempo. No es suficiente con probar los protocolos de seguridad y los algoritmos de cifrado. Una revisión debe cubrir especificación, diseño, aplicación, código fuente, funcionamiento, y todo lo demás. Así como la prueba funcional no puede demostrar la ausencia de errores, una revisión de seguridad no puede demostrar que el producto sea realmente seguro.[3]

Pese a la urgente necesidad de proteger la información, existen empresas que se conforman con "probar a medias" la seguridad de su red de datos por no ver afectado su aspecto económico. Otras empresas, por el contrario, implementan estudios de seguridad

---

[1] Instituto Nacional de Estadística e Informática. Seguridad en Redes De Datos. http://www.aebius.com

[2] Tesis "Seguridad Informática: Sus Implicancias e Implementación" http://www.cfbsoft.com.ar

[3] "Seguridad de la Información" http://ww.monografias.com

computacional e invierten en la adquisición de software de scaneo de detección de vulnerabilidades, con la confianza de evitar problemas cuyas consecuencias son irreparables.

3. JUSTIFICACIÓN Y ALCANCES DEL PROYECTO

Son muchos los riesgos a los que diariamente se enfrentan las empresas de hoy, debido al gran auge de la globalización de la Web y al impresionante desarrollo tecnológico; es por ello que algunas empresas han tomado conciencia de ello y están desarrollando documentos y directrices para obtener el adecuado uso de sus recursos tecnológicos, teniendo en cuenta recomendaciones que garanticen su mayor provecho, evitando la manipulación indebida, procurando así mantener un alto compromiso para permitir crecer como empresa y mantenerse de forma competitiva en el mercado.

Se plantea en esta investigación el análisis de desempeño de software de detección de vulnerabilidades con el fin de establecer unas pautas que apoyen la decisión del tipo de software que se debe adquirir para proteger la red de datos.

Este análisis requiere de un estudio profundo que garantice la planeación, organización, coordinación; con el fin de dirigir y controlar las actividades relacionadas a mantener y garantizar la integridad física de los recursos activos y pasivos de la red, así como su correcto funcionamiento.

Al presentar

- Los métodos más comunes que se utilizan hoy en día para perpetrar ataques a la seguridad informática y que violan de manera directa la confidencialidad, integridad y disponibilidad de la información
- Las armas que se pueden implementar para la defensa
- Pautas que orienten la decisión sobre la metodología de estudio se seguridad computacional que se debe implementar
- El análisis y la comparación de desempeño de algunas herramientas software de scaneo de red de datos
- Pautas para discernir entre aplicar una u otra herramienta de scaneo

la organización o empresa además de tener una herramienta de ayuda para saber cómo los pueden atacar y desde donde, tendrá la guía para determinar su situación actual, detectar vulnerabilidades, diseñar e implantar una solución de seguridad en su red.

4. MARCO TEORICO

4.1. SEGURIDAD INFORMATICA

Diariamente las empresas se enfrentan a un gran desarrollo tecnológico, y a su vez tienen que estar preparadas para tener el control de las posibles violaciones a la seguridad de su información. Por esta razón algunas empresas están invirtiendo recursos para adecuar su infraestructura computacional, asumiendo el alto compromiso de crecer como empresa y mantenerse de forma competitiva en el mercado cambiante.

La información es un valor clave para cualquier institución ya sea pública o privada. La carencia de información o una información defectuosa pueden llevar la empresa a la ruina. Para que la empresa tenga éxito debe tener una información de calidad.

El objetivo de la seguridad computacional es garantizar la privacidad de la información y la continuidad del servicio, tratando de minimizar la vulnerabilidad de los sistemas ó de la información contenida en ellos, así como también proteger las redes privadas y sus recursos mientras que se mantienen los beneficios de la conexión a una red pública o a una red privada.

Hablar de seguridad implica relacionarse con una serie de términos o conceptos básicos los cuales se detallaran en este documento, con el fin de proporcionar un mejor entendimiento del tema.

4.1.1. PROPIEDADES DE LA SEGURIDAD INFORMÁTICA

- **Confidencialidad.** Se puede hablar de confidencialidad en los sistemas cuando la información manipulada por este, no es disponible ni puesta al descubierto para usuarios, entidades o procesos no autorizados.

- **Integridad.** un sistema posee la propiedad de integridad si garantiza que los datos manipulados por éste no son alterados o destruidos por usuarios, entidades o procesos no autorizados.

- **Disponibilidad.** Un sistema posee la propiedad de disponibilidad si, la información está accesible en el momento en que así lo deseen los usuarios, entidades o procesos autorizados.

- **Autenticación.** Un sistema posee la propiedad de autenticación cuando permite verificar si la persona que esta accediendo al sistema es realmente quien debe hacerlo o es un extraño

4.1.2. SEGURIDAD COMPUTACIONAL

Es el conjunto de políticas y mecanismos que nos permiten garantizar la confidencialidad, la integridad y la disponibilidad de los recursos de un sistema. Para determinar dicho aspecto se tiene en cuenta los siguientes conceptos:

- **Amenaza.** Circunstancia o evento que puede causar daño violando la confidencialidad, integridad o disponibilidad.
- **Vulnerabilidad.** Es la debilidad de un sistema informático que permite que sus propiedades de sistema seguro sean violadas. La debilidad puede originarse en el diseño, la implementación o en los procedimientos para operar y administrar el sistema; en el argot de la seguridad computacional una vulnerabilidad también es conocida como un hoyo.
- **Riesgo**. Es la pérdida potencial derivada de las amenazas y vulnerabilidades; y busca representar las pérdidas en términos cuantitativos y/o cualitativos.

Dentro del concepto de seguridad se distingue la Seguridad Física y la Seguridad Lógica:

- **Seguridad Física.** Comprende aspectos del hardware, la manipulación del mismo, así como también el ambiente en el cual se van a instalar los equipos de computo.
- **Seguridad Lógica.** La seguridad lógica comprende el aspecto de los sistemas, tanto operativos como de información.

También existen otros causantes de violación a la seguridad computacional como:

- **Hacker.-** Es una persona con conocimientos de electrónica e informática, que prueba y modifica las cosas que tiene entre sus manos y se pasa largas horas pensando en ello. Es capaz de buscar programas en la red y ejecutarlos.
- **Los crackers.**- Los Crackers en realidad son Hackers, pero con intenciones que van mas allá de experimentar en casa, que se dedica única y exclusivamente a destruir sistemas electrónicos o informáticos.
- Alcanza satisfacción cuando logra destruir un sistema y esto se convierte en una obsesiva compulsión y aprovecha la oportunidad para demostrar al mundo de sus conocimientos y que son capaces quebrantar los sistemas de seguridad.

4.1.3. MÉTODOS DE PROTECCIÓN

En las organizaciones, las políticas son el primer paso que se da para entrar en el ambiente de seguridad, pues reflejan su voluntad de hacer algo que permita detener un posible ataque antes de que éste suceda.

4.1.3.1. Sistemas De Detección De Intrusos. Permiten analizar y buscar en los sistemas, acciones o eventos que puedan considerarse sospechosos, con respecto a la información.

4.1.3.2. Sistemas Orientados A Conexión De Red. Herramientas como los cortafuegos (Firewall) y los Wrappers, permiten monitorear las redes en busca de acciones no permitidas pudiendo orientar e informar a los administradores de red de lo que está sucediendo, para que este tome las decisiones y correctivos que sean necesarios.

4.1.3.3. Sistemas De Análisis De Vulnerabilidades. Estos analizan sistemas en busca de vulnerabilidades conocidas anticipadamente. La desventaja de estos sistemas es que pueden ser utilizados tanto por personas autorizadas como por personas que busquen acceso no autorizado al sistema. Dentro de este tipo de herramientas podemos encontrar el *commview*, *Nextray* entre otros*.*

4.1.3.4. Sistemas De Protección A La Privacidad De La Información. Existen una serie de Herramientas que utilizan criptografía para asegurar la información de tal forma que sólo pueda ser visible por quien tenga autorización para verla. Tiene gran aplicabilidad en la comunicación entre dos entidades. Dentro de este tipo de herramientas podemos situar a Secure Sockets Layer (SSL) y los Certificados digitales tipo X.509.

4.1.4. BENEFICIOS DE LA SEGURIDAD COMPUTACIONAL

La seguridad de un sistema computacional, trae consigo una serie de beneficios inmediatos que permite que la organización trabaje sobre una plataforma confiable, observándose de lo siguiente:

- • Mayor productividad.
- • Mayor motivación del personal.
- • Compromiso con la organización.
- • Mejores relaciones laborales.

4.1.5. CAUSAS DE LA INSEGURIDAD INFORMATICA

- Crecimiento acelerado de las redes empresariales
- El gran auge de la *Internet*
- Confiarse demasiado de la seguridad con que se cuenta actualmente
- No hacer un seguimiento continuo a las políticas de seguridad existentes
- No observar lo que los usuarios realizan continuamente
- Compartir recursos sin restricción alguna

4.2. TIPOS DE VIOLACIONES A LA SEGURIDAD INFORMATICA

Existen cuatro categorías generales de amenazas o ataques que son:

- **Interrupción:** un recurso del sistema es destruido o se vuelve no disponible. Este es un ataque contra la disponibilidad. Ejemplos de este ataque son la destrucción de un elemento hardware, como un disco duro, cortar una línea de comunicación o deshabilitar el sistema de gestión de ficheros.
- **Intercepción:** una entidad no autorizada consigue acceso a un recurso. Este es un ataque contra la confidencialidad. La entidad no autorizada podría ser una persona, un programa o un ordenador.
- **Modificación:** una entidad no autorizada no sólo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la integridad. Ejemplos de este ataque son el cambio de valores en un archivo de datos, alterar un programa

para que funcione de forma diferente y modificar el contenido de mensajes que están siendo transferidos por la red.

- **Fabricación:** una entidad no autorizada inserta objetos falsificados en el Sistema. Este es un ataque contra la autenticidad. Ejemplos de este ataque son la inserción de mensajes espurios en una red o añadir registros a un archivo.

4.2.1. ATAQUES ACTIVOS

Estos ataques implican algún tipo de modificación del flujo de datos transmitidos. Entre estos ataques se encuentran:

- Suplantación de la identidad
- Captura de mensaje, enviándolo nuevamente (consignación bancaria)
- Modificación de mensajes
- Degradación fraudulenta del servicio

4.2.2. ATAQUES PASIVOS

El atacante únicamente escucha o monitoriza la comunicación sin alterarla, únicamente con el fin de obtener la información que está siendo transmitida. Sus objetivos son la intercepción de datos y el análisis de tráfico, que puede consistir en:

* Obtención del origen y el destinatario
* Control de volumen de tráfico
* Control de las horas habituales

4.2.3. TIPOS DE ATAQUES A LA REDES DE INFORMACION

Los insiders (empleados disconformes o personas externas con acceso a sistemas dentro de la empresa) utilizaban sus permisos para alterar archivos o registros. Los outsiders (personas que atacan desde afuera de la ubicación física de la organización) ingresaban a la red simplemente averiguando un password válido.

A través de los años se han desarrollado formas cada vez más sofisticadas de ataque para explotar "agujeros" en el diseño, configuración y operación de los sistemas. Esto permitió a los nuevos atacantes tomar control de sistemas completos, produciendo verdaderos desastres que en muchos casos llevó a la desaparición de aquellas organizaciones o empresas con altísimo grado de dependencia tecnológica (bancos, servicios automatizados, etc.).

Estos nuevos métodos de ataque han sido automatizados, por lo que en muchos casos sólo se necesita conocimiento técnico básico para realizarlos. El aprendiz de intruso tiene acceso ahora a numerosos programas y scripts de numerosos "hacker" bulletin boards y web sites, donde además encuentra todas las instrucciones para ejecutar ataques con las herramientas disponibles.

Los métodos de ataque descriptos a continuación están divididos en categorías generales que pueden estar relacionadas entre sí, ya que el uso de un método en una categoría

permite el uso de otros métodos en otras. Por ejemplo: después de crackear una password, un intruso realiza un login como usuario legítimo para navegar entre los archivos y explotar vulnerabilidades del sistema. Eventualmente también, el atacante puede adquirir derechos a lugares que le permitan dejar un virus u otras bombas lógicas para paralizar todo un sistema antes de huir.

4.2.3.1. Eavesdropping Y Packet Sniffing. Muchas redes son vulnerables al eavesdropping, o la pasiva intercepción (sin modificación) del tráfico de red. En Internet esto es realizado por packet sniffers, que son programas que monitorean los paquetes de red que están direccionados a la computadora donde están instalados. El sniffer puede ser colocado tanto en una estación de trabajo conectada a red, como a un equipo router o a un gateway de Internet, y esto puede ser realizado por un usuario con legítimo acceso, o por un intruso que ha ingresado por otras vías. Existen kits disponibles para facilitar su instalación.

Este método es muy utilizado para capturar loginIDs y passwords de usuarios, que generalmente viajan claros (sin encriptar) al ingresar a sistemas de acceso remoto (RAS). También son utilizados para capturar números de tarjetas de crédito y direcciones de e-mail entrante y saliente. El análisis de tráfico puede ser utilizado también para determinar relaciones entre organizaciones e individuos.

4.2.3.2. Snooping Y Downloading. Los ataques de esta categoría tienen el mismo objetivo que el sniffing, obtener la información sin modificarla. Sin embargo los métodos son diferentes. Además de interceptar el tráfico de red, el atacante ingresa a los documentos, mensajes de e-mail y otra información guardada, realizando en la mayoría de los casos un downloading de esa información a su propia computadora.

4.2.3.3. Tampering O Data Diddling. Esta categoría se refiere a la modificación desautorizada de los datos, o al software instalado en un sistema, incluyendo borrado de archivos. Este tipo de ataques son particularmente serios cuando el que lo realiza ha obtenido derechos de administrador o supervisor, con la capacidad de disparar cualquier comando y por ende alterar o borrar cualquier información que puede incluso terminar en la baja total del sistema en forma deliberada. O aún si no hubo intenciones de ello, el administrador posiblemente necesite dar de baja por horas o días hasta chequear y tratar de recuperar aquella información que ha sido alterada o borrada.

Como siempre, esto puede ser realizado por insiders u outsiders, generalmente con el propósito de fraude o dejar fuera de servicio un competidor.

Son innumerables los casos de este tipo como empleados (o externos) bancarios que crean falsas cuentas para derivar fondos de otras cuentas, estudiantes que modifican calificaciones de exámenes, o contribuyentes que pagan para que se les anule la deuda por impuestos en el sistema municipal.

Múltiples web sites han sido víctimas del cambio de sus home page por imágenes terroristas o humorísticas, o el reemplazo de versiones de software para download por otros con el mismo nombre pero que incorporan código malicioso (virus, troyanos).

La utilización de programas troyanos esta dentro de esta categoría, y refiere a falsas versiones de un software con el objetivo de averiguar información, borrar archivos y hasta tomar control remoto de una computadora a través de Internet como el caso de Back Orifice y NetBus, de reciente aparición.

4.2.3.4. Spoofing. Esta técnica es utilizada para actuar en nombre de otros usuarios, usualmente para realizar tareas de snoofing o tampering. Una forma común de spoofing, es conseguir el nombre y password de un usuario legítimo para, una vez ingresado al sistema, tomar acciones en nombre de él, como puede ser el envío de falsos e-mail.

El intruso usualmente utiliza un sistema para obtener información e ingresar en otro, y luego utiliza este para entrar en otro, y en otro. Este proceso, llamado *Looping*, tiene la finalidad de evaporar la identificación y la ubicación del atacante. El camino tomado desde el origen hasta el destino puede tener muchas estaciones, que exceden obviamente los límites de un país. Otra consecuencia del *looping* es que una compañía o gobierno pueden suponer que están siendo atacados por un competidor o una agencia de gobierno extranjera, cuando en realidad están seguramente siendo atacado por un insider, o por un estudiante a miles de Km. de distancia, pero que ha tomado la identidad de otros.

El looping hace su investigación casi imposible, ya que el investigador debe contar con la colaboración de cada administrador de cada red utilizada en la ruta, que pueden ser de distintas jurisdicciones.

Los protocolos de red también son vulnerables al spoofing. Con el IP spoofing, el atacante genera paquetes de Internet con una dirección de red falsa en el campo From, pero que es aceptada por el destinatario del paquete.

El envío de falsos e-mail es otra forma de spoofing permitida por las redes. Aquí el atacante envía a nombre de otra persona e-mail con otros objetivos.
Muchos ataques de este tipo comienzan con ingeniería social, y la falta de cultura por parte de los usuarios para facilitar a extraños sus identificaciones dentro del sistema. Esta primera información es usualmente conseguida a través de una simple llamada telefónica.

4.2.3.5. Jamming O Flooding. Este tipo de ataques desactivan o saturan los recursos del sistema. Por ejemplo, un atacante puede consumir toda la memoria o espacio en disco disponible, así como enviar tanto tráfico a la red que nadie más puede utilizarla.

Muchos ISPs (proveedores de Internet) han sufrido bajas temporales del servicio por ataques que explotan el protocolo TCP. Aquí el atacante satura el sistema con mensajes que requieren establecer conexión. Sin embargo, en vez de proveer la dirección IP del emisor, el mensaje contiene falsas direcciones IP (o sea que este ataque involucra también spoofing). El sistema responde al mensaje, pero como no recibe respuesta, acumula buffers con información de las conexiones abiertas, no dejando lugar a las conexiones legítimas.

Muchos *host* de Internet han sido dados de baja por el "ping de la muerte", una versión-trampa del comando ping. Mientras que el ping normal simplemente verifica si un sistema esta enlazado a la red, el ping de la muerte causa el reboot o el apagado instantáneo del equipo.

Otra acción común es la de enviar millares de e-mail sin sentido a todos los usuarios posibles en forma continúa, saturando los distintos servers destino.

4.2.3.6. Caballos De Troya. Consiste en introducir dentro de un programa una rutina o conjunto de instrucciones, por supuesto no autorizadas y que la persona que lo ejecuta no conoce, para que dicho programa actúe de una forma diferente a como estaba previsto (Por ejemplo: Formatear el disco duro, modificar un fichero, sacar un mensaje, etc.).

4.2.3.7. Bombas Lógicas. Este suele ser el procedimiento de sabotaje mas comúnmente utilizado por empleados descontentos. Consiste en introducir un programa o rutina que en una fecha determinada destruirá, modificara la información o provocara el cuelgue del sistema.

4.2.3.8. Ingeniera Social. Básicamente convencer a la gente de que haga lo que en realidad no debería. Por ejemplo llamar a un usuario haciéndose pasar por administrador del sistema y requerirle la password con alguna excusa convincente. Esto es común cuando en el Centro de Cómputo los administradores son amigos o conocidos.

4.**2.3.9. Difusión De Virus.** Si bien es un ataque de tipo tampering, difiere de este porque puede ser ingresado al sistema por un dispositivo externo (diskettes) o través de la red (e-mail u otros protocolos) sin intervención directa del atacante. Dado que el virus tiene como característica propia su auto reproducción, no necesita de mucha ayuda para propagarse a través de una Lan o Wam rápidamente, si es que no esta instalada una protección antivirus en los servidores y estaciones de trabajo.

Existen distintos tipos de virus, como aquellos que infectan archivos ejecutables (.exe, .com, .bat, etc.) y los sectores de *boot-particion* de discos y diskettes, pero aquellos que causan en estos tiempos mas problemas son los macro-virus, que están ocultos en simples documentos o planilla de cálculo, aplicaciones que utiliza cualquier usuario de PC, y cuya difusión se potencia con la posibilidad de su transmisión de un continente a otro a través de cualquier red o Internet. Y además son multiplataforma, es decir, no están atados a un sistema operativo en particular, ya que un documento de MS-Word puede ser procesado tanto en un equipo Windows 3.x/95/98, como en una Macintosh u otras.

Cientos de virus son descubiertos mes a mes, y técnicas más complejas se desarrollan a una velocidad muy importante a medida que el avance tecnológico permite la creación de nuevas puertas de entrada. Por eso es indispensable contar con una herramienta antivirus actualizada y que pueda responder rápidamente ante cada nueva amenaza.

El ataque de virus es el más común para la mayoría de las empresas, que en un gran porcentaje responden afirmativamente cuando se les pregunta si han sido víctimas de algún virus en los últimos 5 años.

4.2.3.10. Explotación De Errores De Diseño, Implementación U Operación. Muchos sistemas están expuestos a "agujeros" de seguridad que son explotados para acceder a archivos, obtener privilegios o realizar sabotaje. Estas vulnerabilidades ocurren por variadas razones, y miles de "puertas invisibles" han sido descubiertas en aplicaciones de software, sistemas operativos, protocolos de red, browsers de Internet, correo electrónico y toda clase de servicios en Lan o Wan.
Sistemas operativos abiertos como Unix tienen agujeros mas conocidos y controlados que aquellos que existen en sistemas operativos cerrados, como Windows NT. Constantemente encontramos en Internet avisos de nuevos descubrimientos de problemas de seguridad (y herramientas de hacking que los explotan), por lo que hoy también se hace indispensable contar con productos que conocen esas debilidades y pueden diagnosticar un servidor, actualizando su base de datos de *tests* periódicamente.

Además de normas y procedimientos de seguridad en los procesos de diseño e implementación de proyectos de informática.

4.2.3.11. Obtención De Passwords, Códigos Y Claves. Este método (usualmente denominado cracking), comprende la obtención "por fuerza bruta" de aquellas claves que permiten ingresar a servidores, aplicaciones, cuentas, etc. Muchos passwords de acceso son obtenidos fácilmente porque involucran el nombre u otro dato familiar del usuario, que además nunca la cambia. En este caso el ataque se simplifica e involucra algún tiempo de prueba y error. Otras veces se realizan ataques sistemáticos (incluso con varias computadoras a la vez) con la ayuda de programas especiales y "diccionarios" que prueban millones de posibles claves hasta encontrar el password correcto.

Es muy frecuente crackear un password explotando agujeros en los algoritmos de encriptación utilizados, o en la administración de las claves por parte la empresa.

Por ser el uso de passwords la herramienta de seguridad mas cercana a los usuarios, es aquí donde hay que poner énfasis en la parte "humana" con políticas claras (como se define una password?, a quien se esta autorizado a revelarla?) y una administración eficiente (cada cuanto se están cambiando?)

No muchas organizaciones están exentas de mostrar passwords escritas y pegadas en la base del monitor de sus usuarios, u obtenerlas simplemente preguntando al responsable de cualquier PC, cual es su password?.

4.2.3.12. Eliminar El Blanco. Ping Mortal. Algunos ataques eliminan el blanco en lugar de inundarlo con trabajo. Un ejemplo de este tipo es el ping mortal, un paquete ping ilícitamente enorme, que hace que el equipo de destino se cuelgue. Muchas implementaciones de routers, la mayoría de los Unix y todas las versiones de Windows se mostraron vulnerables a este ataque cuando se lo descubrió por primera vez hace un par

de años. A pesar de que los vendedores lanzaron parches de inmediato, hay todavía cantidades significativas de hosts "no corregidos" en las redes de producción (en especial, las que corren bajo el Windows 95).
TCP/IP permite un tamaño máximo de paquete de 64 kilobytes (KB, este máximo está dividido en piezas mucho más pequeñas a través de protocolos de capas más bajas, como *Ethernet* o *token ring*, pero dentro de una computadora, paquetes mucho más grandes son posibles). Para lidiar con un paquete de 64 KB, la cola TCP/IP asigna un *buffer* en memoria de 64 KB. Al recibir una cantidad ilícitamente grande de información, como un ping mortal, el *buffer* del equipo de destino se desborda y el sistema se puede colgar.

4.2.4. OTRAS FORMAS DE COLGAR UN EQUIPO

4.2.4.1 Land Attack. Otro método para colgar un equipo es el denominado Land attack, en el que se genera un paquete con direcciones IP y puertos de fuente y destino idénticos. Existen diferentes variantes para este ataque. Una de ellas usa idénticas direcciones IP de fuente y destino, pero no números de puertos.
Fue esta variación la que utilizó NSTL contra el primer par de productos testeados y los dos identificaron el tráfico como un land attack. El tercer producto que se probó, el Netranger, de Cisco, identificó a un land attack solamente (y correctamente) cuando ambas direcciones y números de puerto eran idénticos. El ingeniero de Cisco agregó enseguida una nueva regla, que detectaba a los paquetes con direcciones idénticas nada más. Una vez más, esto pone de manifiesto la importancia de saber qué es lo que se debe buscar.

4.2.4.2 Supernuke. Un ataque característico de los equipos con Windows es el Supernuke (llamado también a veces Winnuke), que hace que los equipos que escuchan por el puerto UDP 139 se cuelguen. Netbios es un protocolo integral para todas las versiones en red de Windows. Para transportar Netbios por IP, Microsoft ideó el Windows Networking (Wins), un esquema que enlaza el tráfico Netbios a puertos TCP y UDP 137, 138 y 139. Al enviar a estos puertos fragmentos UDP, se pueden arruinar equipos Windows que no estén arreglados o disminuir la velocidad del equipo durante un largo tiempo.
En cuanto a la inundación ICMP, todos los IDS reconocieron a los ataques Supernuke.

4.3. POLITICAS DE SEGURIDAD

Una política de seguridad informática, consiste en definir las expectativas de una institución respecto al uso adecuado de los recursos de la red, así como especificar los procedimientos precisos para prevenir y responder a los actos que van en contra de la seguridad.

El desarrollo de una política de seguridad comprende la identificación de los activos organizativos, evaluación de amenazas potenciales, la evaluación del riesgo,

implementación de las herramientas y la tecnología disponible para hacer frente a los riesgos y el desarrollo de una política de eficiente.

Para definir políticas de seguridad en una entidad, se deben tener en cuenta ciertos aspectos como:

- Identificar que cosas en la institución merecen protección
  - Software: programas fuente, utilidades, programas de diagnostico, sistemas operativos.
  - Hardware: computadores y equipos utilizados en la red
  - Datos: copias de seguridad, registro de auditorias, bases d datos.
- Hacer una valoración del riesgo: determinar que se necesita proteger, examinar riesgos y valorarlos por niveles de seguridad.
- Establecer áreas y grados de riesgo: crear conciencia en los usuarios a cerca del riesgo que corre la información
- Evaluar la dependencia de los sistemas de información
- Evaluar su impacto a nivel institucional
- Determinar la información que tiene un alto costo financiero
- Establecer prioridades en cuanto a seguridad a corto y largo plazo

4.3.1. TIPOS DE POLITICAS

- Política Militar: Están Definidas para proteger información, mantener la confidencialidad, especialmente de documentos para combatir los peligros del espionaje.
- Política Comercial: Están se diseñan con el fin de controlar fraudes y errores, buscan mayormente la integridad que la confidencialidad.
- Política Financiera: Se basa en agrupar la información en clases de conflicto de interés.

4.3.2. OTROS ELEMENTOS DE LAS POLITICAS

- Responsabilidad: Implica mantener un registro de los eventos relevantes que hallan ocurrido en contra de la seguridad. (tipo de evento, momento en que ocurrió y persona que lo realizo).
- Custodio: Usuario a quien se le ha encomendado vigilar la seguridad de un recurso.
- Fronteras: Es una técnica utilizada por los sistemas operativos para limitar la acción de un programa sospechoso.
- Puede ser útil en disminuir la proliferación de virus.
- Consistencia: Las políticas deben ser consistentes desde el punto de vista del modelo con el mundo real.
- Otra forma de consistencia es que la Política no entre en contradicción en sus propias reglas o propiedades.

4.4. TECNICAS DE SEGURIDAD EN LAS REDES

4.4.1. WRAPPERS

Permite que el administrador fortalezca la seguridad de un programa más de lo que podría hacer el programa por si mismo. Es un programa que es usado para controlar el acceso de un segundo programa.

Un programa muy conocido para brindar seguridad en maquinas *unix* es el *Tcp_Wrappers*, con el que se pueden controlar los puertos de software de un equipo como el *telnet*, *pop3*, *ftp*, *finger* etc.

4.4.2. FIREWALL

Es un sistema o grupo de sistemas que decide que servicios pueden ser acezados desde el exterior (Internet) a una red privada, por quienes pueden ser ejecutados estos servicios y también que servicios pueden correr los usuarios de la Intranet hacia el exterior (Internet).

El *firewall* a diferencia del *router* no direcciona información solamente la filtra, desde el punto de vista de seguridad el *firewall* delimita el área de defensa y seguridad de la organización.

Se puede definir como una colección de componentes colocados entre dos redes, que en conjunto poseen las siguientes propiedades:

- Todo el tráfico de afuera hacia adentro, y viceversa, debe pasar por el *firewall*.
- Sólo tráfico autorizado, como establecido previamente en las políticas de la organización, puede pasar a través del *firewall*.
- El *firewall* mismo es invulnerable

El *firewall* permite accesos selectos de usuarios, autentificando mediante métodos robustos a los usuarios antes de conceder el acceso a recursos vitales, garantizando así, la confidencialidad e integridad en comunicaciones sobre medios inseguros, además, Provee seguridad en los contenidos, evitando los virus.

Desde el punto de vista de política de seguridad, el *firewall* delimita el perímetro de defensa y seguridad de la organización. El diseño de un firewall, tiene que ser el producto de una organización conciente de los servicios que se necesitan, además hay que tener presentes los puntos vulnerables de toda red, los servicios que dispone como públicos al exterior de ella.

4.4.2.1. Beneficios del *Firewall*

- Maneja el acceso entre dos redes, de no ser así, todos los *host* de la Intranet estarían expuestos a ataque de host remotos desde Internet.
- Es el punto ideal para monitorear la seguridad de la red y generar alarmas de ataques.
- Es el lugar ideal para almacenar los NAT.
- Permite llevar estadísticas del uso del ancho de banda consumido.

4.4.2.2 Tipos de Firewall

4.4.2.2.1. packet filter (filtro de paquetes). Se basa en el tratamiento de los paquetes IP a los que aplica unas reglas de filtrado que le permiten discriminar el tráfico según nuestras indicaciones. Se implementa mediante un *router* con dos interfaces de red, uno de cara al exterior y otro al interior, podría utilizarse cualquier computador con 2 tarjetas de red. Los filtros se establecen a nivel de direcciones ip tanto de origen como de destino.

4.4.2.2.2. *firewall* a nivel de aplicación. Es el extremo opuesto a los filtros de paquetes, en lugar de basarse en el filtrado de paquetes trata los servicios por separado, utilizando el código adecuado para cada uno. Es probablemente el sistema mas seguro, ya que no necesita tratar complicadas listas de acceso y centraliza en un solo punto la gestión de servicios y además permite controlar y recoger información de todos y cada uno de los servicios por separado

4.4.2.2.3 *firewall* a nivel de circuitos. Se basan en el control de las conexiones TCP y actúan como si fuesen un cable de red, por un lado reciben las solicitudes de conexión a un puerto TCP; y por otro establecen la conexión con el destino deseado.

4.4.2.2.4 *firewall* basado en certificados digitales. Son extremadamente seguros y con una gran funcionalidad, no han sido muy populares debido a que hasta hace poco no existían distribuidores de certificados universales.

4.4.3. CRIPTOGRAFÍA

Es el arte de construir códigos secretos para Cambiar la información por símbolos sin sentido para las partes que no tienen el permiso de ver la información como es en realidad. Es una ciencia que se ocupa principalmente de conseguir que nuestros mensajes sean comprensibles exclusivamente para aquellos que nosotros deseemos e inteligibles para el resto de la Humanidad, aplicando para ello procedimientos matemáticos o claves. El texto inicial, el de partida, recibe el nombre de texto claro. El que resulta de aplicarle el algoritmo criptográfico, es el texto cifrado.

Los sistemas de cifrado simétrico, son mas débiles que los sistemas de cifrado asimétrico, esto es así por que tanto emisor como receptor deben emplear la misma clave, tanto para el proceso de encriptación como para el proceso de desencriptacion, de esta forma la clave debe ser enviada por algún medio de transmisión. Los sistemas de cifrado asimétrico, al emplear distintas claves, permite el uso de medios de transmisión poco seguros.

Los objetivos de la criptografía son: mantener la confidencialidad del mensaje haciendo que la información permanezca oculta o secreta, garantizando tanto la autenticidad del mensaje como el origen y destino del mismo.

4.4.4. PROXY

Los servidores proxy proporcionan el acceso a una red insegura para determinados protocolos de aplicación a través de un host con doble acceso. El programa del cliente se comunica con el servidor proxy en lugar de hacerlo directamente con el servidor real situado en la red insegura.

El servidor proxy es el encargado de evaluar las solicitudes del cliente y decide cuáles deja pasar y cuáles no. Si una petición es aceptada, el proxy se comunica con el servidor real en nombre del cliente (el término proxy significa representante) y lleva a cabo las peticiones de servicio del cliente al verdadero servidor y transmite las respuestas de éste de nuevo al cliente.

Es importante realizar las conexiones a través de un proxy junto con algún método de restricción de tráfico IP entre los clientes y los servidores en la red insegura, como un router con filtrado de paquetes o un host con doble acceso que no enrute paquetes. Si hay conectividad a nivel IP entre clientes y servidores de la red insegura, los clientes pueden saltarse el servidor proxy y producirse ataques desde el exterior.

Al utilizar un servidor proxy, los usuarios pueden conectarse de una forma más o menos transparente a un servidor de la red externa de forma directa sin que se den cuenta que están pasando por una máquina intermedia, el servidor proxy. No obstante, esto requiere re-configuraciones en los programas cliente (navegador HTTP, cliente FTP, etc.).

4.4.4.1. Ventajas De Los *Proxies*

- Acceso directo a la red externa: Los usuarios pueden conectarse de una forma mas o menos transparente a un servidor de la red externa sin que se den cuenta que están pasando por un maquina intermedia.
- *Loggins* del sistema: Gracias a que los servidores *Proxy* trabajan a nivel de aplicación resulta fácil generar *logs* o monitorizar las conexiones de los usuarios a cada tipo de servicio.

5. HERRAMIENTAS SOFTWARE PARA DETECCIÓN DE VULNERABILIDADES

Durante los últimos años ha crecido de forma dramática el número de herramientas de seguridad para Windows y UNIX, siendo incluso más sorprendente el hecho de que la mayoría de ellas estén disponibles gratuitamente en Internet.

Linux y sus aplicaciones son software libre: han de ser distribuidas con el código fuente al alcance de quien quiera y puede ser modificado libremente, se distribuyen las modificaciones con la misma licencia (GPL).

Existen diferentes categorías principales de herramientas, las que escanean hosts desde el mismo host, las que escanean otros hosts e informan acerca del tipo de SO que están ejecutando (utilizando una técnica llamada huella TCP-IP), los servicios disponibles, etc., estando en la cima de la cadena alimenticia las herramientas de intrusión que intentan ejecutar exploits, e informan acerca de los que funcionaron y los que no, y finalmente la categoría de exploits.

A continuación se presenta la descripción de algunas herramientas de software libre para detectar vulnerabilidades en una red:

5.1. ESCANEO DE HOSTS

5.1.1. TIGER

El Tiger es obsoleto, la Universidad de Agricultura y Mecánica de Texas solía requerir que un host UNIX pasara por el tiger antes de que se le permitiera conectar a la red desde fuera. Se puede conseguir en: ftp://net.tamu.edu/pub/security/TAMU/

5.1.2. SBSCAN

El SBScan es un scanner basado en host, busca una variedad de problemas como ficheros rhosts malignos, puertos abiertos, cuentas de contraseñas, y escanea la red buscando otro tipo de inconveniencias. El SBScan ya no se encuentra en desarrollo, pero está disponible en: http://www.haqd.demon.co.uk/

5.1.3. CHECK.PL

Check.pl es un interesante programa que comprueba los permisos de ficheros y directorios, e informa acerca de cualquier cosa sospechosa o de los "malos" (setuid, setgid, directorios con permiso de escritura, etc.). Muy útil pero tiende a encontrar un exceso de falsos positivos. Se encuentra disponible en: http://opop.nols.com/proggie.html

5.2. ESCANEO DE RED

5.2.1. STROBE

EL clásico escaneador de puertos TCP de alta velocidad. El Strobe es una de las más veteranas herramientas de escaneo de puertos, simplemente se intenta conectar a varios puertos de una máquina(s) e informa del resultado (si existe). Es simple de utilizar y muy rápido, pero no tiene ninguna de las características que tienen los nuevos escaners de puertos. El Strobe se encuentra disponible desde la mayoría de las distribuciones, como parte de la misma, o como un paquete contribuido, los fuentes se encuentran disponibles en: ftp://suburbia.net/pub/

5.2.2. NMAP

Es una herramienta de exploración de red y escáner de seguridad con posibilidades de detección remoto del Sistema Operativo del sistema auditado. Sus características son innumerables y altamente útiles. Es seguramente la mejor herramienta de su clase, por sus rápidas actualizaciones, por la gente que colabora y por su gran base de datos de fingerprints recogidas por gente de todo el mundo. Nmap adoptó técnicas efectivas de localización de fingerprint del proyecto QueSo y otras altamente efectivas que hacen de esta utilidad sin duda la mejor. El Nmap es una herramienta de escaneo más reciente y con más características. Tiene técnicas avanzadas, como las huellas TCP-IP, un método por el cual se examinan los paquetes TCP-IP devueltos, y se deduce el SO del host basándose en diferentes peculiaridades presentes en todas las pilas TCP-IP. El Nmap soporta un número de métodos de escaneo, desde los escaneos normales de TCP (simplemente tratar de abrir una conexión como es habitual) hasta escaneos clandestinos (stealth scanning) y escaneos SYN semi-abiertos (fenomenales para cascar pilas TCP-IP inestables). Este es indiscutiblemente uno de los mejores programas de escaneo de puertos disponibles, ya sea comercial o de cualquier otro tipo. Nmap se encuentra disponible en: http://www.insecure.org/nmap/index.html.

5.2.3. PORTSCANNER

Portscanner es un pequeño escaneador de puertos que tiene diferentes niveles de salida, lo cual le hacen sencillo de utilizar en scripts y por humanos. Es código abierto y de uso gratuito, se puede conseguir en: http://www.ameth.org/~veilleux/portscan.html

5.2.4. Queso

Averigua el Sistema Operativo en una máquina remota viendo las respuestas TCP.El Queso no es un scanner per se, pero informa con un grado de exactitud bastante alto el SO que está utilizando un host remoto. Utilizando una variedad de paquetes tcp válidos e inválidos para probar el host remoto, compara la respuesta con una lista de respuestas conocidas para diferentes sistemas operativos, y te dirá qué SO está ejecutando el host remoto. Se puede conseguir desde: http://www.apostols.org/projectz/queso/

5.2.5. FPORT

El netstat mejorado de Foundstone. Fport reporta todos los puertos, TCP/IP y UDP abiertos en la máquina en la que se está ejecutando y muestra que aplicación abrió cada puerto y sus aplicaciones asociadas. Solo funciona para windows. Se puede conseguir desde: http://www.thegrid.net/gravitino/products.html

5.2.6. OTROS

HERRAMIENTA	DIRECCION
MNS	http://www.thegrid.net/gravitino/products.html
BRONC BUSTER VS. MICHAEL	http://www.thegrid.net/gravitino/products.html
JACKSON	http://www.thegrid.net/gravitino/products.html
LEET SCANNER	http://www.thegrid.net/gravitino/products.html
SOUP SCANNER	http://members.tripod.de/linux_progz/
NETWORK SUPERSCANNER	

5.3. ESCANEO DE INTRUSOS

5.3.1. NESSUS

Nessus es relativamente nuevo pero rápidamente se está perfilando como una de las mejores herramientas de escaneo de intrusos. Tiene una arquitectura cliente/servidor, el servidor se ejecuta en Linux, FreeBSD, NetBSD y Solaris, y los clientes están disponibles para Linux, Windows y hay un cliente Java. La comunicación entre el servidor y el cliente va cifrada, para mayor seguridad, todo en un hábil trozo de código. El Nessus soporta escaneo de puertos, y ataques, basado en direcciones IP o nombres de host(s). También puede buscar a través de la información DNS de la red, y atacar hosts los relativos, según tu interés. Nessus es relativamente lento en modo ataque, lo cual no es sorprendente. Sin embargo, en la actualidad cuenta con 200 ataques y un lenguaje de plug-ins. Está disponible en: http://www.nessus.org/

5.3.2. SAINT

Security Administrator´s Integrated Network (Herramienta de red integrada para el administrador de Seguridad). Corre exclusivamente sobre UNIX. Saint solía ser gratuito y "open source", pero ahora es un producto no-libre. Saint es el sucesor de Satan, un escáner de seguridad de red hecho famoso por los medios de comunicación hace unos años (había serias preocupaciones de que los malos acabaran con Internet haciendo uso de el). Saint también utiliza una arquitectura cliente /servidor, pero utiliza un interfaz www en lugar de un programa cliente. El Saint produce una salida muy fácil de leer y entender, graduando por prioridad los problemas de seguridad (aunque no siempre de forma correcta) y también soporta módulos de escaneo añadidos, lo cual le hace muy flexible. Entre sus capacidades incluidas estan el escaneo a través del firewall, actualización de comprobaciones de seguridad de los boletines del CERT & CIAC, 4 niveles de gravedad 8rojo, amarillo, marrón y verde) y con un buen interface HTML. Saint está disponible en: http://www.wwdsi.com/saint/

5.3.3. CHEOPS

"Swiss-army-knife" de red basado en GTK. tiene un interface más simple que la mayoría de las utilidades, mapea local o remotamente redes y puede mostrar tipos de Sistema Operativo de las máquinas de la red. Si bien no es un escáner per se, es útil para detectar el SO de un host y manejar un gran número de hosts rápidamente. El Cheops es un "entorno de red" con esteroides, construye una imagen de un dominio, o bloque IP, qué está ejecutando cada host y así sucesivamente. Es extremadamente útil para preparar un escaneo inicial, pues se pueden localizar elementos interesantes (Impresoras HP, routers Ascend, etc) con rapidez. El Cheops está disponible en: http://www.marko.net/cheops/

5.3.4. FTPCHECK / RELAYCHECK

Dos sencillas utilidades que escanean en busca de servidores ftp y de correo que permitan retransmisión, bueno para hacerse una idea de qué usuarios molestos están instalando servicios que no deberían (o simplemente desconfigurándolos), disponible desde: http://david.weekly.org/code/

5.3.5. SARA

Asistente de Búsqueda para el Auditor de Seguridad, Security Auditor's Research Assistant, es una herramienta de funciones similares a las de SATAN y Saint. El SARA soporta múltiples hilos para escaneos más rápidos, guarda sus datos en una base de datos para facilidad de acceso y genera interesantes informes en HTML. SARA es de uso gratuito y está disponible en: http://home.arc.com/sara/

5.3.6. BASS

El BASS, "Escáner de Seguridad de Auditoría Masiva", "Bulk Auditing Security Scanner", permite escanear internet en busca de una variedad de exploits bien conocidos. En esencia, fue una prueba del concepto de que Internet no es seguro. Se puede conseguir en: http://www.securityfocus.com/data/tools/network/bass-1.0.7.tar.gz

5.3.7. FRAGOUTE

La peor pesadilla de los IDS. Fragroute intercepta, modifica y rescribe eltráfico de sakuda, implementando la mayoría de los ataques descritos en el "IDS Evasión Paper" de Secure Networks. Entre sus características, se encuetra un lenguaje de reglas simple para retrasar, duplicar, descartar, fragmentar, superponer, imprimir, reordenar, segmentar, especificar source-routing y otras operacionanes más en todos los paquetes salientes destiados a un host en particular, con un mínimo soporte de comportamiento aleatorio o probabilístico. Esta herramienta fue escrita de buena fe para ayudar en el ensayo de sistemas de detección de intrusión,firewalls y comportamiento básico de implementaciones TCP/IP. Al igual que Dsniff y Libdnet, esta excelente herramienta fue escrita por Dug Song.

5.4. ESCANEO DE CORTAFUEGOS

5.4.1. FIREWALK

Firewalk es un programa que utiliza un estilo similar al traceroute para escanear un cortafuegos e intentar deducir las reglas impuestas en ese cortafuegos. Al enviar paquetes con diferentes tiempos de vida y ver dónde mueren o si son rechazados, se puede engañar al cortafuegos para que revele sus reglas. No existe una defensa real contra esto, aparte de denegar silenciosamente los paquetes en lugar de enviar un mensaje de rechazo, lo cual con suerte revelará menos cosas. El Firewalk se encuentra disponible en: http://www.packetfactory.net/firewalk/

6. ANÁLISIS DE DESEMPEÑO DE HERRAMIENTAS DE DETECCIÓN DE VULNERABILIDADES

9.1. DESCRIPCION

El software utilizado para las pruebas es bajado de Internet y para analizar su desempeño, se dispone de una red de 25 computadores. Se pretende analizar el escaneo de vulnerabilidades, la detección de intrusos y el firewall, sin entrar en detalle sobre el funcionamiento de cada una de las herramientas usadas.

6.2. ESCANEO DE VUNERABILIDADES

El Escáner puede identificar routers, switches, firewalls, hubs, servidores de impresión de archivos, y hosts. También puede identificar los sistemas operativos y servicios de la red que corren en los dispositivos identificados en la red. Esta información constituye un mapa electrónico eficaz en el cual el Escáner fácilmente puede basar la explotación para confirmar las vulnerabilidades.

6.2.1. RESULTADO

Rango de Direcciones	192.168.255.248 - 192.168.255.248
Servicios Frecuentes	NetBIOS : netbios-ss Info-Status : ms-browser-service-election Info-Status : ms-domain-name
Vulnerabilidades confirmadas	SSH RSAREF2 Buffer Overflow.

- Las versiones de ssh y sshd compiladas con la opción with-rsaref son vulnerables al desbordamiento del *buffer*. Esta vulnerabilidad hace posible ejecutar los comandos arbitrarios tales como el código de la librería RSAREF2, lo que implica la ejecución de comandos remotos como root.

Rango de Direcciones	192.168.255.245 - 192.168.255.245
Servicios Frecuentes	Web : http-ssl Windowing : xwindow Mail : pop

Puerto Abierto / Protocolo TCP	25, 110, 111, 143, 443, 6000
	111
Puerto Abierto / Protocolo UDP	Desconocido
S.O.	Recon:RPC.portmapper-Active:Vp. Recon:RPC.rstatd-Active:Vp.
Vulnerabilidades Detectadas	

- El portmapper es un servicio para la Llamada del Procedimiento Remota (RPC). No corre en puertos fijos, al iniciar escoge un puerto libre al azar y lo registra en el portmapper. Los programas que utilizan este servicio le preguntan al portmapper para la dirección del puerto que ellos desean usar. El portmapper es así un blanco importante para los ataques de reconocimiento. Esta vulnerabilidad ayuda al atacante para determinar el tipo y versión del servicio de RPC y puede servirle como preludio a un ataque.

- El rstatd es un servicio que retorna el rendimiento estadístico del *Kernell* de una *unix* en que se este corriendo. Esta vulnerabilidad permite al atacante identificar sistemas ociosos que pueden ser fáciles de atacar sin que se descubra.

Rango de Direcciones	192.168.254.242 - 192.168.254.242
Servicios Frecuentes	Info-Status:chargen, daytime, discard, echo, finger, rpc-portmapper, rpc-rquotad, rpc-statd, rpc-rstatd, rpc-rusersd, rpc-sprayd, syslog, tcpmux time Data-Transfer:tftp File-Sharing:rpc-mountd, rpc-nfs, rpc-nlockmgr Mail:smtp Net-Management:dhcp, dns Other:printer, rpc-walld, ttdbserverd Remote-Access:rlogin, telnet, Exec:rexec, xec:rsh Web:http Windowing:xwindows
Puerto Abierto / Protocolo TCP	1, 7, 9, 13, 19, 21, 23, 25, 37, 53, 79, 80, 111, 513, 514, 515, 2049, 6000
Puerto Abierto / Protocolo UDP	67, 69, 111, 514, 2049
S.O.	OS workstation:unix:sgi:irix

Vulnerabilidades Detectadas	Recon:RPC.sprayd-Active:Vp:1112 Recon:RPC.rusersd-Active:Vp:1122 Recon:RPC.rstatd-Active:Vp:1124 Recon:RPC.rquotad-Active:Vp:1109 Recon:RPC.portmapper-Active:Vp Recon:Finger.Active:Vp:101 Access:RPC.statd-Active:Vp:1113 Denial:RPC.walld-Active:Vp:1123 Access:Rsh.Active:Vp:1003 Y rlogin

- **Recon:RPC.sprayd-Active:Vp:1112.** El demonio del sprayd es un servidor que graba el número de paquetes recibidos del programa y responde al cliente con esta información. Esto es usado frecuentemente para la solución de problemas. Esta vulnerabilidad brinda la información del estado de la red al intruso.

- **Recon:RPC.rusersd-Active:Vp:1122.** Los usuarios remotos y locales de unix pueden usar este servicio para obtener información detallada sobre otras cuentas de usuarios activos en este servicio. Esta vulnerabilidad permite obtener nombres de usuario válidos y sus contraseñas.

- **Recon:RPC.rstatd-Active:Vp:1124.** Este servicio retorna el rendimiento estadístico del Kernell de una unix en que se este corriendo. Esta vulnerabilidad permite que un atacante accese al rstatd remotamente, descubrir los programas ociosos sin que se descubra.

- **Recon:RPC.rquotad-Active:Vp:1109.** El *daemon* del rquotad se usa para proporcionar información sobre el uso del disco y límites en NFS del *filesystems* montado. Esta vulnerabilidad puede facilitar un ataque de negación del servicio identificando qué sistemas del archivo están llegando a su nivel máximo.

- **Recon:RPC.portmapper-Active:Vp.** El *portmapper* es un servicio para la Llamada del Procedimiento Remota (RPC). Este servicio no corre en puertos fijos, cuado se inicial el servicio, este escoge un puerto libre al azar y lo registra en el *portmapper*. Los programas que utilizan este servicio le preguntan al *portmapper* para la dirección del puerto que ellos desean usar. El *portmapper* es así un blanco importante para los ataques de reconocimiento.
- **Consecuencias.** Un atacante puede determinar el tipo y versión del servicio de RPC y pude servirle como preludio a un ataque. Hay también ataques de la red que involucran un rechazo de servicio al portmapper o pueden usar las vulnerabilidades en el portmapper para subvertir la seguridad del sistema.

- **Recon:Finger.Active:Vp:101.** El demonio finger proporciona información sobre las cuentas de usuario en un sistema unix. El finger puede permitir a los asaltantes remotos obtener cuentas de usuarios. Esta vulnerabilidad permite obtener cuentas de usuarios y contraseñas.

- **Access:RPC.statd-Active:Vp:1113.** The stat daemon provides crash and recovery control for the NFS file locking services. Esta vulnerabilidad permite ejecutar órdenes o archivos de sistema.

- **Denial:RPC.walld-Active:Vp:1123.** *Walld* es un servicio que acepta mensajes de *Brodcast*. Esta vulnerabilidad permite saturar de tráfico y negar el servicio.

- **Access:Rsh.Active:Vp:1003 Y rlogin.** El servicio del rsh permite ejecución de ordenes remotas en rede locales. Este servicio puede permitir acceso sin la autenticación si el usuario está incluido en el archivo de .rhosts o el archivo de hosts.equiv. Esta vulnerabilidad permite que un intruso gane acceso y ejecute órdenes remotamente.

6.3. ESCANEO DE VUNERABILDADES CON NMAP

El software Nmap trabaja inicialmente con paquetes ICMP para escanear puertos, y luego introduce tráfico TCP para generar actividad "Stealth".

IP 192.168.254.246

PUERTOS TCP	ESTADO	SERVICIO
22	Abierto	Ssh
25	Abierto	Smtp
53	Abierto	Domain
80	Abierto	http
139	Abierto	netBios-sns
443	Abierto	https
3306	Abierto	mysql
4444	Abierto	krb524
6000	Abierto	x11
8081	Abierto	blakice-icecap

IP 192.168.254.244

PUERTOS TCP	ESTADO	SERVICIO
21	Abierto	ftp
25	Abierto	Smtp
27	Abierto	Nsw-fe
42	Abierto	nameserver
80	Abierto	http

110	Abierto	pop-3
111	Abierto	sunrpc
119	Abierto	nntp
135	Abierto	loc-srv
139	Abierto	netbios-ssn
143	Abierto	imap2

6.4. DETECCIÓN DE INTRUSOS

6.4.1. ESCANEO DE PUERTOS.

Se trabaja con el software superscan bajado de Internet. Se simula el envío de paquetes a un rango de direcciones IP de la red para detectar los puertos abiertos.

6.4.2. PAQUETES ICMP.

Se trabaja con el software Tosser bajado de Internet. Se simula el envío de paquetes ICMP.

6.4.3. DETECCIÓN DE SISTEMA OPERATIVO.

Se trabaja con el software nmapwin. Se detecta el Sistema Operativo, se escanea los puertos.

6.4.4. ATAQUES POR FUERZA BRUTA.

Se trabaja con el software Brutus A2 bajado de Internet. Mediante comandos del servicio Telnet, http y POP3 para encontrar las contraseñas de los usuarios.

6.4.5. ATAQUES POR DESBORDAMIENTO DE BUFFER.

Se trabaja con el software Anonimail. Se simula el envío de correos electrónicos anónimos.

6.5. FIREWALL

Un firewall es una aplicación o sistema que actúa como intermediario entre dos redes restringiendo la comunicación entre ellos mediante un conjunto de reglas definidas. Esto es, software o hardware, que con la intención de aumentar la seguridad de una comunicación, la filtra. Generalizando se pueden distinguir dos métodos de firewalling:

- Filtros de paquetes: filtros a nivel de transporte y red. Por ejemplo: si se desea que desde la red se acceda a webs pornográficas, se puede rechazar las peticiones de conexión a direcciones como www.playboy.com.

- Proxies: filtros a nivel de transporte, red y aplicación, principalmente este último. Existen proxies para gran variedad de servicios como X, FTP, TELNET, etc... Normalmente también incluyen otras funciones, como: caché (muy frecuente en proxies web y ftp) y autentificación. Por ejemplo: un proxy FTP puede denegar las peticiones 'GET', permitiendo así solo navegar por FTPs.

Se encontró diversidad de interconexión entre una red privada e Internet:

- Proxies tradicionales: la intranet no tiene conexión directa a Internet. Para salir se conectó al router (en este caso del tipo 'dual homed gateway'), en el que existen proxies para acceder a ciertos servicios de Internet. En el router puede correr Squid (un proxy web de Linux). Los paquetes de la intranet nunca llegarán a Internet ni viceversa. Los clientes de la intranet necesitan una configuración adicional para usar los servicios del router para acceder a Internet.

- Proxies transparentes: este escenario es igual al de los proxies tradicionales salvo que no necesitan una configuración adicional de los clientes de la intranet.

- Masquerading (enmascaramiento): la intranet sale a Internet a través del router. En este caso, solo el router dispone de conexión a Internet, y para que la intranet pueda acceder el router, usa una característica especial del kernel: masquerade. Esta técnica consiste en sustituir en las cabeceras de los paquetes a enviar a Internet, la dirección de los ordenadores de la intranet por la del router conectado a Internet, así todos los ordenadores de la intranet aparecen como si fueran el router, pero para ellos todo es como si realmente estuvieran conectados.
- Red pública: los ordenadores de la intranet disponen de IPs reales de Internet, a la que salen a través del router, que actúa de firewall filtrando el tráfico que va hacia ellos.

El firewall que hace el NAT se llama gateway, pues tiene múltiples tarjetas de red, una por cada red a proteger los bastion hosts. Antiguamente era el tramo inseguro que iba desde el router hasta el firewall con direcciones ip públicas en Internet actualmente nadie pone sus servidores directamente en Inet con IPs públicas ahora la DMZ también está protegida tras el firewall y los servidores son vistos desde fuera a través de Nat.

7. CONCLUSIONES

- Los productos evaluadores de vulnerabilidades, también conocidos como rastreadores de vulnerabilidad, son desarrollos que efectúan auditorias de seguridad sobre los sistemas en uso, buscando cuales son los puntos en que son vulnerables a cierto tipo de ataques.

- Los productos evaluadores de vulnerabilidades pueden trabajar de dos maneras para localizar e informar las vulnerabilidades a la seguridad que encuentran.

- Los productos evaluadores de vulnerabilidades como rastreo o escaneo pasivo, revisa la configuración del sistema, en lo que se relaciona con los permisos de los archivos, la propiedad declarada en los archivos críticos, la configuración de los paths y busca configuraciones que la experiencia ha demostrado que generan problemas de seguridad.

- Los productos evaluadores de vulnerabilidades como escaneo o rastreo activo, recrea una serie de ataques conocidos realizados por hackers y registra los resultados de los mismos. Algunos de estos productos también desarrollan el crackeo de los archivos de contraseñas para descubrir aquellas incorrectas o débiles que podrían ser fácilmente adivinadas por los hackers. Finalmente el producto registra sus hallazgos en pantalla o en algún otra forma de informe.

- Los productos evaluadores de vulnerabilidades son una parte valiosa de cualquier programa de administración de la seguridad de los sistemas en cualquier organización. Le permite a los responsables delimitar o establecer una línea de seguridad en todo nuevo sistema. Permiten llevar a cabo auditorías periódicas de seguridad para determinar la salud del sistema en un momento preciso. Muchos proveen la capacidad de desarrollar análisis diferenciados, archivando los resultados de los rastreos, para luego compararlos con los siguientes realizados sobre los archivos e informando cuando aparece una nueva vulnerabilidad o un cambio inesperado.

- Cuando un IDS es reactivo, detectando ataques mientras o después que estos ocurren, el Análisis de Vulnerabilidades es proactivo, determinando la susceptibilidad a los ataques antes de que las redes sean explotadas. Con una detección de vulnerabilidades a tiempo, las compañías pueden tomar acciones correctivas ante de que los ataques dañinos a sus redes puedan concretarse.

- El análisis de Vulnerabilidades ha sido conducido por años con técnicas como los test de penetración anuales o trimestrales. En la actualidad, con las soluciones automatizadas para Análisis de Vulnerabilidades, las organizaciones pueden detectar y eliminar las vulnerabilidades frecuentemente a un costo razonable, cerrando la ventana de exposición de las redes.

- El Análisis de Vulnerabilidades trabaja en conjunto con los antivirus, firewalls e IDS.

- El Análisis de Vulnerabilidades identifica vulnerabilidades potenciales antes de que puedan ser explotadas y los sistemas de detección de intrusos notifican cuando una actividad anómala ocurre. Estos dos elementos tienen una acción sinergizante: el Análisis de Vulnerabilidades habilita la identificación y cierre de huecos de seguridad obvios mientras que el sistema de detección de intrusos tiene menores lugares que chequear.

- Los cuatro pilares de la seguridad en redes son: Antivirus, firewall, Sistemas de Detección de intrusos y Detección de vulnerabilidades.

- Un sistema de detección de intrusiones monitorea una variedad de fuentes de información de los sistemas, haciendo un análisis de esos datos de varias maneras. El primero y más común, compara la información obtenida con la existente en las grandes bases de datos de identificaciones de ataques, donde están almacenadas las formas posibles conocidas de los intentos de evitar o sobrepasar las protecciones de seguridad. El segundo, bucea en aquellos problemas relacionados con usuarios autorizados que intentan exceder los límites de sus permisos, como por ejemplo un empleado administrativo que intenta acceder a los registros donde figuran los salarios de los gerentes.

- Algunos sistemas de detección de intrusiones realizan un análisis matemático sobre la información, buscando individualizar patrones de actividad normal que podrían no caer en aquellas dos primeras categorías, como por ejemplo un acceso que ocurre en momentos del día o en días inusuales u una cantidad no acostumbrada de ingresos fallidos.

- El corta fuego es una herramienta de seguridad informática basada en la aplicación de un sistema de restricciones y excepciones. Es el equivalente en seguridad física de una organización, a instalar una cerca alrededor de una propiedad con un custodio en la puerta de acceso. Logra mantener a la mayoría de las personas alejadas, pero no puede necesariamente decir qué es lo que está pasando dentro del complejo.

- Los sistemas de detección de intrusiones son los equivalentes a los equipos de video multisensores y a los sistemas de alarma contra ladrones. Estos guardan la información que reciben y se la analiza para detectar patrones de comportamiento sospechoso. Operan de una forma parecida a la del custodio al recorrer los puestos y de las imágenes que vienen de las cámaras de seguridad para su examen y sólo en algunos casos resuelven el problema que detectan.

- Teniendo instalado un firewall es necesario implementar un sistema de detección de intrusos debido a que la mayoría de las pérdidas originadas en incidentes de seguridad informática, se deben al abuso cometido por usuarios internos. Los

sistemas de detección de intrusiones, y no los cortafuego, son los capaces de detectar esta categoría de violación de la seguridad.

- Los firewall están sujetos a diversos tipos de ataques. Los dos más importantes son los ataques "tunneling" (salteo de barreras) y los ataques basados en las aplicaciones. Los ataques que saltean las barreras surgen de las propiedades del protocolo que se utiliza en la red.

- Los firewall filtran los paquetes y permiten su pasaje o los bloquean por medio de una tabla de decisiones basadas en el protocolo de la red. Las reglas verifican contra una base de datos que determina si está permitido un protocolo determinado y, si lo está, permite el paso del paquete. Esto se transforma en un problema cuando un atacante enmascara el tráfico que debería ser analizado por el corta fuego y lo encapsula dentro de paquetes correspondientes a otro protocolo de la red. Los ataques con base en las aplicaciones se refieren a la práctica de explotar las vulnerabilidades de las mismas, mandándoles paquetes que se comunican directamente con dichas aplicaciones. Por lo tanto, se puede explotar un problema con el software de la Web mandando un comando http que hace que haya demasiado flujo en el buffer de la aplicación. Si el firewall está configurado para dejar pasar el trafico http, el paquete conteniendo el ataque pasará, sin impedimentos.

- La imposibilidad por parte de los firewall de frenar un determinado tipo de ataques, entre los que también cabe mencionar a los populares virus informáticos, no debe ser considerada como fallas sino, como aspectos que escapan a las funcionalidades previstas en el diseño inicial de estas herramientas.

- Se ha invertido mucho en desarrollos para brindar seguridad para la red. Se tiene la identificación y la autentificación, se pidió a los empleados que cifren sus correos electrónicos, se cuenta con corta fuegos, los usuarios generan contraseñas apropiadas y las cambian frecuentemente.

- Aún cuando una organización tenga una muy buena infraestructura de seguridad informática, necesita de la seguridad suplementaria que proveen los sistemas de detección de intrusiones. No importa cuan bien diseñados estén los productos de seguridad, siempre están sujetos a fallas, ya sea por parte del hardware o de las anormalidades del funcionamiento del software con ese hardware o por los problemas de los errores de los usuarios. Los usuarios algunas veces anulan la protección ofrecida por los productos, inhabilitándolos o evitándolos.

- Los sistemas de detección de intrusiones son capaces de monitorear mensajes llegados desde otra parte de la infraestructura de seguridad y de detectar cuando ocurren aquellas fallas. En algunos casos pueden registrar los procesos que ocurren hasta que una persona autorizada los ponga nuevamente en servicio.

- Una limitantes del antivirus es que, aunque, al monitorear los sistemas de archivos y memorias, locales y de servidores en busca de virus, efectivamente detiene los

virus que intentan entrar a las redes y los sistemas, no cierran o eliminan las vulnerabilidades explotadas por los hackers, worms, y ataques automatizados.

- Una limitantes del Firewall es que los cambios en las políticas del firewall pueden exponer vulnerabilidades ocultas.

- Una limitante del Sistema Detección Intrusos es que aunque, notifica a los administradores de posibles intentos de hacking cuando alguna actividad anómala ocurre dentro de la red y/ servidores, pudiendo en ocasiones tomar acciones, no informa a los administradores de vulnerabilidades antes de que sean explotadas. Son propensos a falso positivos, falso negativos y falsas alarmas, además de requerir configuraciones complicadas.

- El Análisis de Vulnerabilidades Permite a las empresas corregir vulnerabilidades antes de que sean explotadas, a través del análisis de dispositivos y sistemas en busca de vulnerabilidades conocidas; identificando su ubicación y proveyendo soluciones verificadas. Informa a los administradores de redes y sistemas de vulnerabilidades y su solución. Pero no informa cuando una intrusión ocurre o cuando algún archivo es infectado por un virus, dejando estas tareas a los IDS's y los antivirus.

- La seguridad informática de los sistemas corporativos requiere otras herramientas de gestión no menos importantes: las políticas de seguridad y el plan de contingencia.

- Las políticas de seguridad de una organización son las normas y procedimientos internos que deben seguir los integrantes de la organización para respetar los requerimientos de seguridad que deseen preservarse.

8. RECOMENDACIONES

Es importante que la empresa adopte una metodología para realizar un estudio de seguridad en un red de datos, para ello pueden considerarse las siguientes etapas:

- Determinación de la situación actual
- Valoración de riesgos
- Diseño de una Solución
- Implantación de la solución
- Administración de la Seguridad

Es importante recordar que varios mecanismos para detectar vulnerabilidades en la red se pueden bajar de Internet y son sencillos de manejar. La detección de vulnerabilidad no garantiza la seguridad de la red, por tanto se deben implementar mecanismos que orienten el manejo conjunto de sistemas de detección de intrusos, firewall y antivirus. Además es necesaria la participación activa de las personas que trabajan a diario con la empresa estableciendo políticas de seguridad y planes de contingencia.

Se debe tener en cuenta que:

- Las políticas de seguridad que adopte la entidad se generan de la estrategia corporativa y se trata de documentos que deben conocer todos los integrantes.

- El plan de contingencia debe contener los procedimientos a seguir ante la aparición de eventualidades significativas que puedan suponer graves consecuencias para la organización.

9. BIBLIOGRAFIA

MAXWELL, Steve. Herramientas para la administración de redes. Red Hat Linux. McGraw-Hill. 2002

BONGHELLO, Cristian. Tesis "Seguridad Informática, sus implicaciones e implementación". 2001.

VILLALÓN, Antonio. Seguridad en UNIX y redes. GNU Free Documentation License. 2002.

INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA. Conceptos sobre seguridad en la información. Lima 2.002.

INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA. Seguridad en redes de datos. Lima 2.002.

CISCO SYSTEMS INC. CISCO SECURE SCANNER. User Guide. 2002.

CISCO SYSTEMS INC. Installing Cisco Secure Scanner For Windows NT. V 2.0

CISCO SYSTEMS INC. Configuring Ipsec Network Security. http://www.ietf.org

BRACHO, Haller. Iptables y el servicio de traducción de direcciones de redes NAT. http:://www.hbracho.Linux .org.ve

LUCENA, Manuel. Criptografía y Seguridad en computadores. Segunda Edición. 2002.

NETWORK ASSOCIATES, INC. User's Guide to CyberCop Scanner Version 2.5. 2000. http://www.nai.com

SECURITY TECHNOLOGIES. Solución de Seguridad Informática Core Force. 2.001

www.nessus.org
www.eeye.com
http://www.snort.org
http://vip.ca.com/channel_emea
http://cyberrecursos.net
http://www.timagazine.net
http://www.aebius.com
http://www.monografias.com
http://www.seguridad.unam.mx
http://www.rediris.es/cert