RECOPILACIÓN Y ANÁLISIS DE TÉCNICAS Y HERRAMIENTAS DE SOFTWARE LIBRE UTILIZADAS PARA EL ESCANEO, INTRUSIÓN Y DEFENSA EN REDES DE COMPUTADORAS Y SU APLICACIÓN EN LA EVALUACIÓN DEL NIVEL DE SEGURIDAD DE LA RED DE DATOS DE LA UNIVERSIDAD AUTÓNOMA DE BUCARAMANGA (UNAB)

JENIFFER ANDREA BENÍTEZ PRADA
JUAN CARLOS DÍAZ GÓMEZ

UNIVERSIDAD AUTÓNOMA DE BUCARAMANGA
FACULTAD DE INGENIERÍA DE SISTEMAS
TELECOMUNICACIONES Y TECNOLOGIAS WEB
BUCARAMANGA
2008

RECOPILACIÓN Y ANÁLISIS DE TÉCNICAS Y HERRAMIENTAS DE SOFTWARE LIBRE UTILIZADAS PARA EL ESCANEO, INTRUSIÓN Y DEFENSA EN REDES DE COMPUTADORAS Y SU APLICACIÓN EN LA EVALUACIÓN DEL NIVEL DE SEGURIDAD DE LA RED DE DATOS DE LA UNIVERSIDAD AUTÓNOMA DE BUCARAMANGA (UNAB)

JENIFFER ANDREA BENÍTEZ PRADA
JUAN CARLOS DÍAZ GÓMEZ

Proyecto de Grado para optar título de
Ingeniero de Sistemas

Director:
ROBERTO CARVAJAL SALAMANCA
Magíster en administración

UNIVERSIDAD AUTÓNOMA DE BUCARAMANGA
FACULTAD DE INGENIERÍA DE SISTEMAS
TELECOMUNICACIONES Y TENOGIAS WEB
BUCARAMANGA
2008

Nota de aceptación:

_____
_____
_____
_____
_____
_____

_____
Firma del director

_____
Firma del jurado

_____
Firma del jurado

Bucaramanga, 23 de Abril de 2008

Dedicatoria

A nuestra familia,
y director de proyecto
Roberto Carvajal Salamanca
por su apoyo y comprensión.

AGRADECIMIENTOS

De manera muy especial a nuestro director de proyecto Roberto Carvajal Salamanca por su incondicional apoyo, paciencia y confianza depositada a lo largo de nuestro trabajo de investigación y desarrollo.

A mis padres Arinda Gómez y José Díaz, mis hermanos Yamil José y Mario Fernando quienes con su colaboración y paciencia hicieron posible la realización de este proyecto.

A mi madre Eleonora Prada Escobar por la capacidad de poder en todo momento hacerme sentir confiada y secundada; por el bagaje aportado, por el esfuerzo no al limite de sus capacidades, sino mucho mas allá de ellas; por el legado trasmitido, que trasciende la existencia misma, producto del esfuerzo diario, que solo el amor de una madre otorga, por acompañarme en mis triunfos que son suyos, y en los momentos difíciles cuando es mi apoyo. Quiero de manera especial agradecer a mi mamá, motivo y razón primordial de mi vida y de mi ser.

Agradecemos también a nuestro amigo Noe Espinza por su constante ayuda, quien fue para nosotros como un asesor, quien nos encaminó por la dirección correcta para la realización del proyecto.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

GLOSARIO

CRON: En el sistema operativo Unix, cron es un administrador regular de procesos en segundo plano (demonio) que ejecuta programas a intervalos regulares (por ejemplo, cada minuto, día, semana o mes). Cron se podría definir como el "equivalente" a Tareas Programadas de Windows.

ESPACIO DE USUARIO: Se refiere a un espacio de aplicación, típicamente en Unix o en sistemas operativos tipo Unix, el cual es externo al núcleo.

EXPLOITS: Un exploit es un programa informático malicioso, o parte del programa, que trata de forzar alguna deficiencia o vulnerabilidad de otro programa (llamadas bugs).

FRAMEWORK: En el desarrollo de software, un framework es una estructura de soporte definida en la cual otro proyecto de software puede ser organizado y desarrollado.

FTP: File Transfer Protocol - protocolo de transferencia de archivos.

GPL: Licencia Pública General. Su propósito es declarar que el software cubierto por esta licencia es software libre y protegerlo de intentos de apropiación que restrinjan esas libertades a los usuarios.

HIJACKING: Hijacking significa "Secuestro" en inglés y en el ámbito informático hace referencia a toda técnica ilegal que lleve consigo el adueñamiento o robo de algo (generalmente información) por parte de un atacante, es por tanto un concepto muy abierto y que puede aplicarse a varios ámbitos, de esta manera

podemos encontramos con el adueñamiento o secuestro de conexiones de red, sesiones de terminal, servicios, módems y un largo etc. en cuanto a servicios informáticos se refiere.

HTTP: HyperText Transfer Protocol - Protocolo de transferencia de hipertexto.
HTTPS. Es la versión segura del protocolo HTTP (HyperText Transfer Protocol, Protocolo de Transferencia de Hipertexto).

IDS: Intrusion Detection System – Sistema De Detección de la Intrusión.

IPSec: Por sus siglas en inglés: Internet Protocol Security.

LAN: Por sus siglas en ingles, Local Area Network.

MALWARE: Es un software que tiene como objetivo infiltrarse en o dañar un computador sin el conocimiento de su dueño.

MODO PROMISCUO: Es aquel modo en el que un computador conectado a una red compartida, tanto la basada en cable de cobre como la basada en tecnología inalámbrica, captura todo el tráfico que circula por ella.

NASL: Nessus Attack Scripting Language - Lenguaje de Scripting de Ataque Nessus por sus siglas en inglés.

NFS: Network File System – Sistema de archivos de red.

OSI: Open System Interconnection - Modelo de referencia de Interconexión de Sistemas Abiertos.

OTP: Por sus siglas en inglés: One-Time Password; traducido al español como: Contraseña de un solo uso.

OVAL: Open Vulnerability and Assessments Language. Es una comunidad internacional de información de seguridad que promueve estándares para el contenido de códigos abiertos y públicos disponibles sobre seguridad, para estandarizar la transferencia de esta información a través de todo el espectro de las herramientas y de los servicios de seguridad.

PKI: Public Key Infrastructure - Infraestructura de clave pública.

PSI: Refiérase a Política de Seguridad Informática.

RADIUS: Por sus siglas en inglés: Remote Access DIAN-In User Service; traducido al español como: Servicio De Usuario Con Acceso Remoto Por Marcación.

RCF: Request For Comments.

REDES CERRADAS: Red que sólo proporciona conectividad a las partes y sitios conocidos sin necesidad de conectar con redes públicas. Red con ausencia de conectividad exterior.

REDES DE COMPUTADORES: Entiéndase por Red de computadora como un conjunto de computadoras y/o dispositivos conectados por enlaces de un medio físico (medios guiados) ó inalámbricos (medios no guiados) y que comparten información, recursos y servicios, etc.

RPC: Llamada a Procedimiento Remoto.

SANS: Es la más confiada y más grande fuente de información para el entrenamiento y la certificación sobre seguridad en el mundo.

SECURE SOCKET LAYERS (SSL): Protocolo criptográfico que proporciona una comunicación segura en Internet. SSL proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía.

SEGURIDAD GLOBAL: El concepto de red global incluye todos los recursos informáticos de una organización, aún cuando estos no estén interconectados: Redes de área local (LAN), Redes de área metropolitana (MAN), Redes nacionales y supranacionales (WAN), Computadoras personales, minis y grandes sistemas. De manera que, seguridad global es mantener bajo protección todos los componentes de una red global.

SHELL: Es una parte fundamental del sistema operativo, encargada de ejecutar las órdenes básicas para el manejo del sistema. Suelen incorporar características tales como control de procesos, redirección de entrada/salida y un lenguaje de órdenes para escribir programas por lotes o scripts.

SMB: Server Message Block – Bloque de mensajes del servidor.

SOCKET: Un Socket designa un concepto abstracto por el cual dos programas (posiblemente situados en computadoras distintas) pueden intercambiarse cualquier flujo de datos, generalmente de manera fiable y ordenada. Un socket queda definido por una dirección IP, un protocolo y un número de puerto.

SQL: Sequenced Quero Language – Lenguaje de consulta estructurado.

SSH: Secure Shell es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red.

TACACS+: Por sus siglas en inglés: Terminal Access Controller Access Control System Plus; traducido al español como: Sistema Plus De Control De Acceso Al Controlador De Acceso Del Terminal.

UDP 139: NetBIOS Servicio de sesiones.

USENET: Users Network (Red de usuarios), consistente en un sistema global de discusión en Internet, donde los usuarios pueden leer o enviar mensajes (denominados artículos) a distintos grupos de noticias ordenados de forma jerárquica.

VNC: Computación en Red Virtual.

VoIP: Voice over IP, Voz Sobre IP.

WRAPPERS: Es un sistema de red ACL que trabaja en terminales y que se usa para filtrar el acceso de red a servicios de protocolos de Internet que corren en sistemas operativos (tipo UNIX), como ser Linux o BSD.

X WINDOWS SYSTEM: Es el sistema de ventanas desarrollado para dotar de una interfaz gráfica a los sistemas Unix. Este protocolo permite la interacción gráfica en red entre un usuario y una o más computadoras haciendo transparente la red para éste. Generalmente se refiere a la versión 11 de este protocolo, X11, el que está en uso actualmente.

ZONA DESMILITARIZADA O DMZ: Es una red local (una subred) que se ubica entre la red interna de una organización y una red externa, generalmente Internet. 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 (hosts) en la DMZ no pueden conectar con la red interna.

RESUMEN

Las sociedades del presente siglo han sido denominadas “sociedades de la información”, debido a que el gran volumen de datos gestionado es mucho mayor al de las épocas anteriores. Gran parte de la información administrada por las organizaciones, es procesada, almacenada o transmitida, haciendo uso de diferentes tecnologías informáticas, por consiguiente, la seguridad de dichas tecnologías es un tema de crucial importancia para su progreso y supervivencia.

El rápido crecimiento de Internet ha sido fundamental para que el tema de seguridad informática cobre vital importancia en el uso de sistemas informáticos conectados. Cuando un computador se conecta a Internet, dispone de toda una serie de posibilidades, sin embargo, también está expuesto a diferentes tipos de ataque clasificados en: Interrupción, interceptación, modificación y fabricación. Adicionalmente, los protocolos de comunicación como TCP/IP no fueron concebidos teniendo en cuenta aspectos de seguridad, convirtiéndose estos dos factores en las principales causas de la inseguridad en la redes de computadores.

El presente trabajo de grado se enfoca el estudio de los aspectos que integran el concepto de seguridad informática, en el estudio de los principales ataques que sufren las redes de datos de las instituciones universitarias, en el estudio de herramientas de software libre empleadas para detectar y contrarrestar ataques y corregir vulnerabilidades en las redes de datos, que permitan diseñar y realizar pruebas sobre la LAN de la universidad, a fin de diagnosticar el estado actual de la misma en cuanto a seguridad se refiere y proponer correctivos en caso de ser necesarios.

LÍNEA DE INVESTIGACIÓN

Telecomunicaciones y tecnologías Web

PALABRAS CLAVE

Seguridad informática, Vulnerabilidades, Ataques, Amenazas, Sniffer

ABSTRACT

The companies of this century have been called “Information societies” due to they are managing a large volume of information compared to the information managed in the past. In fact, a huge amount of information managed by the companies it is processed, it is stored or it is transmitted using all kind of computer technologies. Therefore, the safety of these technologies has a special importance for its progress and its survival in the computers world.

The growth of the Internet has been crucial for making that the topic of the security in systems has a considerable importance in the use of the computer systems interconnected. When a computer is connected to the Internet, it has a lot of benefits while it is connected to the network; but in the same way, this computer is also exposed to different types of attack classifieds in: interruption, interception, modification and manufacturing. In addition to, the protocols, such as TCP/IP was not designed taking into account security aspects. For those reasons, these two factors are considered like the main causes of the insecurity in the computer networks.

This paper focuses on the study of the main aspects that make up the definition of the computer security through: the study of the major attacks suffered by the data networks of the universities, the study of the free software tools used to detect and to decrease the attacks, and also, to correct the vulnerabilities founded in the UNAB data network for designing and making tests on the LAN, in order to diagnose the current state of the same in the security field and in the same way, to propose the actions for being taken if they result necessaries.

RESEARCH FIELD

Telecommunication and technologies Web

KEY WORDS

Vulnerabilities, threats, computer security, attacks, sniffer

INTRODUCCIÓN

Las redes informáticas, y en especial la red de redes, Internet, ocasionaron que las organizaciones aprovecharan las ventajas y posibilidades que éstas les ofrecen a la hora de gestionar su información. En la actualidad, la mayoría de organizaciones gestionan su información a través del uso de redes informáticas que les permitan procesarla, almacenarla y transferirla, a fin de cumplir con las funciones corporativas de las mismas y llevarlas a ser competitivas dentro del mercado en el que se desenvuelven.

La información es considerada el activo más importante dentro de cualquier organización. Es por tanto, que su proceso de gestión se debe llevar a cabo de manera segura; es decir, que su administración se efectúe a través de redes informáticas que cumplan con requerimientos y estándares básicos de seguridad para garantizarle a la organización, la suficiente confiabilidad sobre el manejo de sus datos e información.

Una red nunca puede llegar a ser considerada como 100% segura. Esto se debe a que en paralelo como avanzan las tecnologías y herramientas en pro de alcanzar estándares altos de seguridad informática, van surgiendo amenazas y herramientas que se encargan de violar e infringir al mismo tiempo las nuevas tecnologías y los nuevos estándares de seguridad. Por consiguiente, la seguridad informática es un tema que día a día cobra más valor para las organizaciones, puesto que éstas buscan crear entornos seguros, los cuales no se vean afectados por la irrupción de los flujos de su información privada y confidencial.

Todas las organizaciones que actualmente tienen implementadas redes informáticas, están enfrentando los retos de seguridad que se les presentan como producto de asumir nuevos avances tecnológicos. La Universidad Autónoma de Bucaramanga (UNAB), pese a estar dotada de una buena infraestructura tecnológica en sus redes, no esta exenta de enfrentar retos de seguridad, ni mucho menos, esta exenta de sufrir ataques a las redes de las cuales dispone. Por consiguiente, con el presente trabajo de grado, se espera dejar un documento que contenga un estudio sobre el nivel de seguridad que tiene la LAN de la Universidad, a través de la realización de "Hardening" o "aseguramiento" de la red mediante el uso de herramientas y aplicaciones de software libre. Del mismo modo, con la realización de este documento, se pretende ilustrar el estado actual del nivel de seguridad de la red mediante la elaboración de un diagnóstico que presente los siguientes aspectos: fortalezas, debilidades y correctivos propuestos para mejorar las debilidades y fallos encontrados en la red, con el objeto de brindar una panorámica general sobre la situación actual del nivel de seguridad de la red institucional.

1. MARCO TEÓRICO

1.1 FUNDAMENTACIÓN BÁSICA DE SEGURIDAD INFORMÁTICA[1]

1.1.1 Panorámica de la seguridad en redes. En la actualidad, lo referente a la seguridad informática ha adquirido gran auge entre las organizaciones, dadas las cambiantes condiciones y las nuevas plataformas computacionales disponibles. La posibilidad de interconectarse a través redes de computadoras, ha abierto nuevos horizontes que permiten explorar más allá de las fronteras de la organización. Esta situación ha evidenciado como consecuencia las amenazas, riesgos y vulnerabilidades a los cuales se deben enfrentar los sistemas computarizados respecto al manejo de la información como elemento clave de toda organización.

El crecimiento exponencial de Internet, ha mostrado el valor de la información como bien que debe protegerse. Sin la protección o la seguridad adecuada de la red, tanto individuos, empresas y gobiernos corren el riego de perder dicho bien.

Para tener más claro a que se hace énfasis cuando se habla se *Seguridad en redes,* a continuación se brindará una definición aproximada y acertada sobre lo que denota su concepto.

Seguridad en redes es mantener bajo protección los recursos y la información con que se cuenta en la red, a través de procedimientos basados en una política de seguridad tales que permitan el control de lo actuado.

[1] Academia de Networking de Cisco Systems: Fundamentos de Seguridad de Redes Especialista en Firewall Cisco. Pearson. Madrid: Educación, S.A. 2005.

La seguridad de las redes, es el proceso a través del cual se protegen los recursos de información digital. Los objetivos básicos de la seguridad son: confidencialidad (secreto), integridad, disponibilidad y autenticación

1.1.2 Seguridad computacional. Con estos objetivos plasmados anteriormente, se puede asegurar que una red cumple con los requisitos mínimos de seguridad a fin de evitar amenazas, vulnerabilidades y riesgos, permitiendo que las organizaciones alcancen todo su potencial.

La seguridad computacional es el conjunto de políticas y mecanismos que permiten garantizar la confiabilidad, integridad y disponibilidad de los recursos de un sistema en red. Para determinar dicho aspecto, enseguida se definirán unos conceptos claves:

Una ***Amenaza*** es un acceso no autorizado a una red o a un dispositivo perteneciente a una red. Comúnmente, las amenazas se mantienen en una organización debido a las ***Vulnerabilidades,*** que son problemas que se pueden presentar como producto de una errónea y mala configuración de hardware o software, un diseño pobre de la red, carencias tecnológicas o el descuido y falta de información del usuario final. Mientras que un ***Riesgo*** se define como la pérdida del potencial derivada de las amenazas y vulnerabilidades; y busca representar las pérdidas en términos cualitativos y/o cuantitativos.

Una red no puede llegar a considerarse 100% segura. Los riesgos a nivel de seguridad no pueden eliminarse o prevenirse completamente, pero si se pueden minimizar en gran medida, gracias a una administración y una valoración eficaz de los posibles riesgos existentes. Un nivel aceptable de riesgo es la cantidad de éste que las organizaciones están dispuestas a asumir. Comúnmente, las

organizaciones asumen determinada cantidad riesgo al realizar la comparación *coste vs. Beneficio* de implementación en medidas de seguridad.

Dentro del concepto de seguridad computacional se hace la distinción de la seguridad física y de 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.

Para que existan violaciones a la seguridad computacional, implícitamente existen personas responsables de ejecutar dichas acciones maliciosas para obtener determinado fin. Entre ellas se destacan:

- **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.

1.1.3 Lógica, tendencias y objetivos de la seguridad de las redes. La seguridad en redes tiene un propósito: Mantener alejados y fuera a los "Enemigos". Esto se traduce al hecho de construir muros fuertes para detener el paso de personas mal intencionadas y crear puertas vigiladas y pequeñas, para salvaguardar bajo control el acceso seguro al personal autorizado. Esta estrategia funciona bien para las redes cerradas, implementadas comúnmente a entornos corporativos. En el pasado la mayoría de redes se diseñaban bajo este esquema ya que se tenía en mente que si no había contacto con el exterior, se garantizaría un entorno de red segura, afirmación que es falsa.

- **Necesidad de seguridad en las redes.** En la actualidad, gracias a la llegada de los PC, las LAN y el mundo exterior representado por Internet, las redes actuales son más abiertas. Dicha situación requiere encontrar el equilibrio entre seguir aislado o abrirse al mundo de las comunicaciones, así como distinguir de aquellos usuarios que acceden a la red ya sea para adquirir beneficios o para hacerle daños a la misma.

Con la llegada de las LAN, los PC e Internet, también ha surgido un gran número de riesgos para la seguridad. Del mismo modo, con el paso del tiempo, y de acuerdo a las necesidades demandas por los usuarios de la red, se han creado nuevas soluciones de seguridad, más transparentes y más flexibles.

La mayoría de personas espera que las medidas de seguridad garanticen lo siguiente:

a. Los usuarios sólo pueden llevar a cabo las tareas autorizadas
b. Los usuarios sólo pueden obtener la información autorizada.
c. Los usuarios no pueden provocar daños en los datos, aplicaciones o entorno operativo de un sistema.

d. El sistema puede rastrear las acciones de un usuario y los recursos de red a los que esas acciones acceden.

La palabra *Seguridad* significa protección frente a los ataques malintencionados de intrusos. La seguridad implica controlar los efectos de los errores y los fallos del equipo.

- **Tendencias que afectan a la seguridad en redes.** Existen numerosas tendencias que incrementan la demanda de redes seguras; entre estas se pueden mencionar:

  a. Acceso inalámbrico.
  b. Incremento de los requisitos de ancho de banda.
  c. Problemas legales.
  d. Preocupaciones por la privacidad.
  e. Falta de personal.

- **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.

  a. *Sistemas de detección de intrusos.* Permiten analizar y buscar en los sistemas, acciones o eventos que puedan considerarse sospechosos, con respecto a la información.

  b. *Sistemas orientados a conexión de red.* Herramientas como los cortafuegos (Firewall) y los Wrappers, permiten monitorear las redes en busca de acciones no permitidas permitiendo orientar e informar a los

administradores de red de lo que está sucediendo, para que este tome las decisiones y correctivos que sean necesarios.

c. *Sistemas de análisis de vulnerabilidades.* 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.

d. *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 se pueden situar a: Secure Sockets Layer (SSL) y los Certificados digitales tipo X.509.

- **Beneficios de la seguridad computacional.** La seguridad computacional brinda una serie de beneficios que les permiten a los usuarios del sistema trabajar bajo una plataforma confiable. Entre estos se destacan:

  a. Mayor productividad.
  b. Mayor motivación del personal.
  c. Compromiso con la organización.
  d. Mejores relaciones laborales.

- **Causas de la inseguridad informática.** Algunas de las causas más comunes de la inseguridad informática son:

  a. Crecimiento acelerado de las redes empresariales.
  b. El gran auge del Internet.

c. Confiarse demasiado de la seguridad con que se cuenta actualmente.
d. No hacer un seguimiento continuo a las políticas de seguridad existentes.
e. No observar lo que los usuarios realizan continuamente.
f. Compartir recursos sin restricción alguna.

- **Tipos de violaciones a la seguridad informática.** Existen cuatro categorías generales de amenazas o ataques que son (ver Figura No. 1):

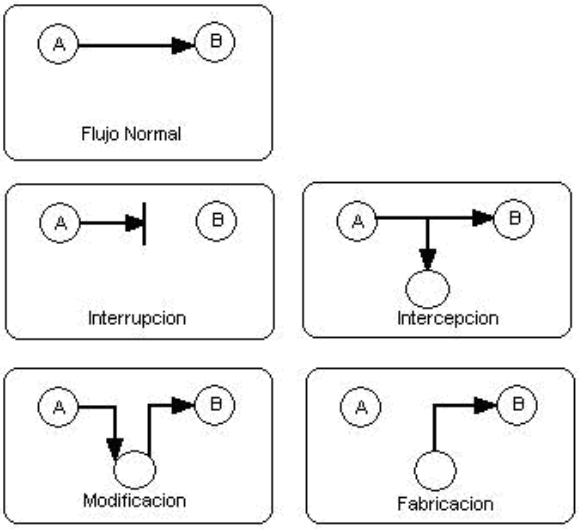
a. *Interrupción:* Un recurso del sistema es destruido o se vuelve no disponible. Este es un ataque contra la disponibilidad. Ejemplos de este ataque son la destrucción de un elemento hardware, como un disco duro, cortar una línea de comunicación o deshabilitar el sistema de gestión de archivos.

b. *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.

c. *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.

d. *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.

Figura 1. Tipos de Violaciones a la Seguridad Informática.



Fuente: Academia de Networking de Cisco Systems: Fundamentos de Seguridad de Redes Especialista en Firewall Cisco. Pearson. Madrid: Educación, S.A. 2005.

- **Objetivos de la seguridad en las redes.** Hay tres objetivos principales en cuanto a seguridad en las redes:

  a. *Confidencialidad.* La confidencialidad se refiere a la protección de los datos ante una revelación no autorizada a terceras partes. Las organizaciones deben hacerse responsables de proteger la privacidad de sus datos (Datos de clientes o Datos internos de la organización).

     La transmisión de información confidencial, debe realizarse de un modo seguro para evitar cualquier acceso no autorizado. La confidencialidad se encarga de exigir que la información sea suministrada únicamente a quienes tienen permisos.

b. *Integridad.* La Integridad se refiere a la certeza de que los datos no son destruidos o modificados de forma no autorizada. La integridad se consigue cuando el mensaje recibido es idéntico al mensaje enviado.

c. *Disponibilidad.* La Disponibilidad es definida como el funcionamiento continuo de los sistemas de computación, teniendo en cuenta los niveles de disponibilidad y el tiempo de inactividad de las aplicaciones. Se dice que una aplicación está disponible cuando todos los componentes proporcionan un servicio continuo.

Los tres objetivos principales de la seguridad en redes parecen muy simples. Sin embargo, los desafíos de asegurar las redes cada vez son mayores debido a las exigencias y necesidades de las organizaciones respecto al manejo de su información. Los administradores deben administrar cuidadosamente las políticas de seguridad para mantener el equilibrio entre el acceso transparente, el uso y la seguridad de la red.

Un acceso transparente a la red se consigue considerando puntos clave como lo son: conectividad, facilidad de uso, rendimiento, manejabilidad y disponibilidad.

En cuanto a seguridad, se deben considerar estos otros puntos: autenticación, autorización, contabilidad, confianza, confidencialidad, integridad de los datos.

1.1.4 Elementos claves de la seguridad en las redes. El uso seguro de las tecnologías de Internet requiere la protección de los datos importantes y de los recursos de la red de las organizaciones ante la corrupción y la intrusión. Una solución de seguridad contiene los siguientes elementos clave:

- *Identidad.* Se refiere a la identificación precisa y correcta de los usuarios, Host, aplicaciones, servicios y recursos de la red. Entre las tecnologías existentes para lograr la identificación en la red se encuentran:

  a. Protocolo RADIUS.
  b. Protocolo TACACS+.
  c. Protocolo Kerberos.
  d. Herramientas OTP.
  e. Certificados digitales.
  f. Tarjetas inteligentes.
  g. Biometría.
  h. Servicios de directorio.

- *Seguridad del Perímetro.* La seguridad en el perímetro brinda los medios para controlar el acceso a las aplicaciones de red, datos y servicios críticos, de modo que sólo los usuarios y la información legítimos puedan pasar a través de la red.

  Esta solución de seguridad se puede lograra mediante:

  a. Firewalls.
  b. Routers y Switches con filtrado de paquetes y capacidad de Firewalls.
  c. Rastreadores de virus.
  d. Filtros de contenidos.

- *Privacidad de los datos.* Para proteger la información de escuchas secretas, lo principal es lograr una comunicación autenticada y confidencial; además del uso de tecnologías de cifrado y de protocolos digitales (IPSec).

- *Administración de la Seguridad.* Para que una red se mantenga segura, es de suma importancia comprobar y monitorear periódicamente su estado a nivel de seguridad. Para conseguir dicho fin, se emplean escaneadores de vulnerabilidades y sistemas de detección de intrusos, para actuar ya sea proactivamente ante una acción o monitorizar y responder ante una falla de seguridad.

- *Administración de políticas.* El crecimiento en cuanto a tamaño y complejidad de las redes evidencia la necesidad de crear e implementar herramientas de administración de políticas, las cuales permiten analizar, interpretar, configurar y monitorizar el estado de seguridad de las redes. En un siguiente apartado, se ampliará y profundizará sobre el tema de políticas de seguridad en las redes.

1.2 INFRAESTRUCTURA Y POLÍTICAS DE SEGURIDAD[2]

1.2.1 La rueda de la seguridad. La "Rueda de la seguridad", es una metodología eficaz destinada a verificar que se han implementado la contramedida frente a las vulnerabilidades en seguridad y que funcionan correctamente. Esta rueda, promueve volver a probar y aplicar las medidas de seguridad actualizadas sobre una base de tiempo continua.

Para iniciar en el proceso de la rueda de seguridad, en primer lugar hay que desarrollar una *Política de Seguridad* que permita la aplicación de medidas en seguridad.

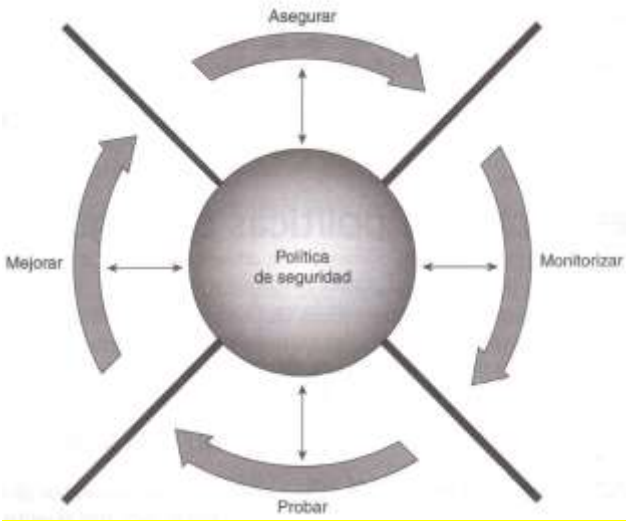
Una política de seguridad debe realizar las siguientes funciones:

[2] Academia Op. Cit., p. 28.

a. Identificar los objetivos en materia de seguridad de la organización.
b. Documentar los recursos que se deben proteger.
c. Identificar la infraestructura de la red con mapas e inventarios actuales.
d. Identificar los recursos críticos que deben protegerse.

Una vez desarrollada la Política de seguridad, se debe convertir en el eje sobre el que se basan los cuatro pasos de la rueda de seguridad (Ver Figura 2):

Figura 2. Rueda de la seguridad.



Fuente: Academia de Networking de Cisco Systems: Fundamentos de Seguridad de Redes Especialista en Firewall Cisco. Pearson. Madrid: Educación, S.A. 2005.

- **Asegurar.** Para impedir y evitar el acceso y la ejecución de actividades no autorizadas, se debe asegurar la red aplicando la política de seguridad e implementar las siguientes soluciones de seguridad:

a. *Autenticación:* Otorgar acceso y privilegios exclusivamente a los usuarios autorizados.

b. *Firewalls:* Filtrar el tráfico de la rede para permitir sólo tráfico y servicios válidos.

c. *Redes Privadas Virtuales (VPN):* Ocultar el contenido del tráfico para evitar que los individuos no autorizados o malintencionados los descubran y puedan hacer uso de él.

d. *Parches para vulnerabilidades:* Aplicar parches o medidas para frenar el ataque por vulnerabilidades conocidas.

- **Monitorizar.** Éste paso consiste en desarrollar e implicar métodos activos y pasivos de detección de violaciones a nivel de seguridad.

  Entre los métodos activos más comunes se encuentra la *auditoria de archivos de registro* a nivel de *Host,* para vigilar el sistema y detectar intrusiones en tiempo real*;* y entre los métodos pasivos se incluye el uso de dispositivos IDS, para detectar automáticamente las intrusiones.

- **Probar.** En esta fase se prueba proactivamente la seguridad de la red. Aquí se ponen en prueba el funcionamiento de las funcionalidades a nivel de seguridad implementadas en la etapa 1 y en la etapa 2. Además, en esta etapa se busca asegurar la seguridad de la red, antes de que ésta sufra algún daño por falencias no detectadas a tiempo. Herramientas como SATAN, Nessus o Nmap, resultan útiles para llevar a acabo la comprobación periódica de las medidas de seguridad de la red.

- **Mejorar.** Esta etapa implica el análisis de los datos recopilados en la etapa de monitorización y prueba, así como el desarrollo e implementación de mecanismos de mejorar que alimenten la política de seguridad y la fase de aseguramiento.

  Para conseguir que una red sea segura en la mayor medida posible, el ciclo de la "Rueda de Seguridad" se debe repetir continuamente, a fin de descubrir nuevas vulnerabilidades y nuevos riesgos, con el objeto de ser mejorados.

1.2.2 Políticas de Seguridad. Una política de seguridad consiste en la especificación de los requisitos de control de acceso a la información y otros elementos de una organización. Estos requisitos de control de acceso determinan qué elementos son accesibles, cómo son accesibles (lectura, escritura, ejecución, etc.), por quién (que personal de la organización y del exterior) y a que horas se podrán hacer, entre otros detalles. Del mismo modo, una PSI establece el canal formal de actuación del personal, en relación con los recursos y servicios informáticos, importantes de la organización.

No se trata de una descripción técnica de mecanismos de seguridad, ni de una expresión legal que involucre sanciones a conductas de los empleados. Es más bien una descripción de los que deseamos proteger y el por qué de ello. Cada PSI es consciente y vigilante del personal por el uso y limitaciones de los recursos y servicios informáticos críticos de la compañía.

Se pueden diferenciar cuatro formas de enfrentarse al problema de la seguridad en una organización. Elegir la adecuada dependerá de diversos aspectos tal como la importancia de los datos que se encaminaran por la red o redes implicadas.

Las políticas de seguridad diseñadas e implementadas para las organizaciones pueden ser clasificadas de la siguiente manera:

a. *Paranoicas:* Todo está prohibido, aun aquello que debería estar permitido; como si no existiera interconexión.

b. *Prudentes:* Todo está prohibido, excepto aquello que se permita de manera explícita.

c. *Permisivas:* Todo está permitido, excepto aquello que se prohíba de manera explícita.

d. *Promiscuas:* Se permite todo, aun aquello que debería prohibirse.

- **Beneficios de una política de seguridad.** Las políticas de seguridad merecen el tiempo y el esfuerzo necesarios para desarrollarlas.

  Una política de seguridad beneficia a una organización en lo siguiente:

  a. Proporciona un proceso para auditar la seguridad actual en la red.

  b. Proporciona una infraestructura de seguridad general para la implementación de seguridad en la red.

  c. Define el comportamiento que ésta o no permitido.

  d. Ayuda a determinar las herramientas y procedimientos necesarios para la organización.

e. Ayuda a alcanzar un consenso en comunicación y define las responsabilidades tanto para usuarios como para administradores.
f. Define un proceso de actuación frente incidente en la seguridad de la red.

g. Habilita la implementación y ejecución de una *seguridad global.*

h. Si es necesario, crea la base para una acción legal.

- **Elementos de una política de seguridad.** Una política de seguridad debe considerar entre otros, los siguientes elementos:

a. Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica. Es una invitación de la organización a cada uno de sus miembros a reconocer la información como uno de sus principales activos así como, un motor de intercambio y desarrollo en el ámbito de sus negocios. Invitación que debe concluir en una posición.

b. Objetivos de la política y descripción clara de los elementos involucrados en su definición.

c. Responsabilidades por cada uno de los servicios y recursos informáticos a todos los niveles de la organización.

d. Requerimientos mínimos para configuración de la seguridad de los sistemas que cobija el alcance de la política.

e. Definición de violaciones y de las consecuencias del no cumplimiento de la política.

f. Responsabilidades de los usuarios con respecto a la información a la que ella tiene acceso.

g. Ofrecer explicaciones acerca de por qué se implemente una política en concreto y no otra, usando un lenguaje libre de tecnicismos que impidan el entendimiento de ella para los miembros de una organización.

- **Desarrollo de una política de seguridad.** Una política de seguridad puede variar desde ser tan sencilla y de tan pocas páginas, como ser tan compleja y con cientos de páginas y especificaciones que la detallan cuidadosamente. Lo cierto es que una política de seguridad está definida correctamente y de la siguiente forma en el RCF 2196:

  "Una política de seguridad es una declaración formal de las reglas por las que deben regirse las personas que tiene acceso a los recursos tecnológicos y de información de una empresa".

  La verdadera seguridad de la red se consigue mediante proceso evolutivo que combine productos y servicios, junto con una política de seguridad integral y un compromiso por parte de los miembros de la empresa, para adherirse a esa política. De hecho, para que una política de seguridad sea apropiada y eficaz, debe tener el apoyo de todos los empleados en todos los niveles de la empresa, para así, configurar todas las funciones de la red, entorno a la política de seguridad elegida.

  Entre los aspectos importantes para la formulación de una política de seguridad se encuentran:

a. Considere efectuar un ejercicio de análisis de riesgos informático, a través del cual valore sus activos, el cual le permitirá afinar las PSI de su organización.

b. Involucre a las áreas propietarias de los recursos o servicios, pues ellos poseen la experiencia y son fuente principal para establecer el alcance y las definiciones de violaciones a la PSI.

c. Comunique a todo el personal involucrado en el desarrollo de las PSI, los beneficios y riesgos relacionados con los recursos y bienes, y sus elementos de seguridad.

d. Recuerde que es necesario identificar quién tiene la autoridad para tomar decisiones, pues son ellos los responsables de salvaguardar los activos críticos de la funcionalidad de su área u organización.

e. Desarrolle un proceso de monitoreo periódico de las directrices en el hacer de la organización, que permita una actualización oportuna de las mismas.

f. No dé por hecho algo que es obvio. Haga explícito y concreto los alcances y propuestas de seguridad, con el propósito de evitar sorpresas y malos entendidos en el momento de establecer los mecanismos de seguridad que respondan a as PSI trazadas.

A continuación se enumeran los atributos o características más importantes que cualquier política de seguridad debe incluir:

Tabla 1. Características importantes de una política de seguridad

Característica	Descripción
Declaración de la autoridad y ámbito	Especifica los patrocinadores de la política de seguridad y las áreas que ésta debe cubrir.
Política de uso aceptable	Especifica lo que la empresa permitirá p no permitirá de acuerdo con su infraestructura de información.
Identificación y política de autenticación	Especifica las tecnologías, equipos, o la combinación de ambas que la empresa utilizará para garantizar que sólo las personas autorizadas podrán acceder a sus datos.
Política de acceso a Internet	Especifica lo que la empresa considera ético y el uso adecuado de sus capacidades de acceso a Internet.
Política de acceso al campus	Especifica cómo los usuarios del campus utilizarán la infraestructura de datos de la empresa.
Política de acceso remoto	Especifica cómo accederán los usuarios remotos a la infraestructura de datos de la empresa.
Procedimiento de manipulación de incidentes	Especifica cómo la empresa creará un equipo de respuesta a los incidentes y los procedimientos que utilizará durante y después de que se produzca un incidente.

Fuente: Academia de Networking de Cisco Systems: Fundamentos de Seguridad de Redes Especialista en Firewall Cisco. Pearson. Madrid: Educación, S.A. 2005.

Toda política de seguridad genera un coste entre productividad del usuario y las medidas de seguridad. La finalidad primordial de cualquier diseño en seguridad, es proporcionar la mayor seguridad con un impacto mínimo en el acceso transparente y la productividad del usuario.

Es por esto, que el diseño y desarrollo de una política de seguridad se fundamente en las necesidades empresariales concretamente. Hay que aclarar que como las empresas cambian constantemente, las políticas de seguridad de las mismas, se deben actualizar y ajustar a las nuevas necesidades, que son producto de nuevas directrices, implementaciones tecnológicas y nuevos recursos a proteger.

- **Niveles de políticas de seguridad.** Normalmente, una política de seguridad tiene dos niveles:

  a. *Nivel de requisitos.* Aquí se define el grado al que deben protegerse los recursos de la red frente a la intrusión o la destrucción, así como la estimación del coste, o las consecuencias, de una falla en la seguridad.

  b. *Nivel de implementación.* Aquí se definen las pautas para implementar la política a nivel de los requisitos, usando la tecnología específica de una forma predeterminada.

La creación de una política de seguridad, implica el cumplimiento secuencial de las dos etapas descritas anteriormente.

1.3 PUNTOS DÉBILES A NIVEL DE SEGURIDAD: CAPAS DEL MODELO OSI[3]

Cada una de las capas del modelo de interconexión de sistemas abiertos OSI, tiene un conjunto de funciones que debe llevar a cabo para que los datos viajen desden un Host origen hasta un Host destino en una red. Por tanto, es posible que maleantes se aprovechen de las falencias intrínsecas presentadas en cada capa para efectuar daños a la red que afecten los recursos de los usuarios.

A continuación se estudia cada una de las capas del modelo OSI:

a. *Capa de Aplicación (Capa 7):* Los ataques efectuados a ésta capa se pueden llevar a cabo utilizando varios métodos. Una de las técnicas más

[3] Academia Op. Cit., p. 28

comunes es explotar los puntos débiles bien conocidos del software que normalmente se encuentra instalado en los servidores (HTTP, Sendmail y FTP). Al aprovecharse de esos puntos débiles, los piratas obtienen acceso a un PC con el permiso de la cuenta que se encarga de ejecutar la aplicación; normalmente se trata de una cuenta con privilegios a nivel del sistema.

El principal problema de los ataques que se presentan en la capa de aplicación consiste en que con frecuencia utilizan puertos que están permitidos a través de un *Firewall* (Puerto TCP 80: navegador Web).

Los ataques realizados en esta capa, nunca pueden eliminarse totalmente. Los puntos débiles que se descubren continuamente, se difunden a través de la comunidad de Internet.

b. ***Capa de Presentación (Capa 6):*** La capa de presentación garantiza que la información que la capa de aplicación de un sistema envía es legible para la capa de aplicación de otro sistema. Si es necesario, la capa de presentación hace la conversión entre varios formatos de datos utilizando un formato común.

Desde el punto de vista de seguridad, cualquier usuario está en capacidad de interceptar y leer esos paquetes de datos con el mínimo esfuerzo, especialmente en un entorno Ethernet CSMA / CD (Acceso múltiple con detección de portadora y detección de colisiones).

Por ende, para proteger los datos, es necesario utilizar el Cifrado. Éste ayuda a mantener la privacidad y seguridad de los mismos, al hacer que éstos sólo sean legibles por el destino que posee la clave de cifrado. Pero sin embargo, con el avance de la tecnología, se necesitan herramientas de cifrado mucho más potentes.

Otro problema de esta capa, se centra en las técnicas de compresión. Troyanos, virus y otros demonios de control comprimidos, que pasan fácilmente sin ser detectados a través de la red entre los *Firewalls,* comprometiendo a *Host* o redes destino después de descomprimirse.

c. ***Capa de Sesión (Capa 5):*** Esta capa establece, administra y termina sesiones entre dos *Host* en comunicación. También sincroniza el diálogo entre las capas de presentación de los dos *Host* y administra su intercambio de datos. Además de la regulación de la sesión, ofrece planes para la eficacia de la transferencia de los datos, la clase de servicio y la información de excepción de los problemas de la capa de sesión, presentación y aplicación.

   Muchos de los protocolos (NFS, SQL, SMB, Xwindows) de esta capa, pueden explotarse para obtener acceso no autorizado a los recursos. Además, a través de estos protocolos, es posible obtener el control raíz del dispositivo.

d. ***Capa de Transporte (Capa 4):*** Esta capa segmenta los datos del sistema *host* emisor y los reensambla como flujo de datos en el sistema *host* receptor, haciendo que establezca, mantenga y termine los circuitos virtuales de la comunicación. Al ofrecer un servicio fiable, se usan la detección y recuperación de errores de transporte y el control del flujo de la información.

   La principal vulnerabilidad presentada en esta capa, se debe al ataque por escaneo de puerto TCP y UDP. Los ataques que se pueden llevar a nivel de segmento son ataques DoS, el *Spoofing* y el *hijacking.*

e. ***Capa de Red (Capa 3):*** Esta capa proporciona conectividad y selección de ruta entre dos sistemas de *host,* que pueden encontrarse en redes geográficamente separadas. Entre los abusos a nivel de paquete se encuentra los escaneadores de *Ping,* el *Sniffing,* ataques DoS, inversión ARP, el *Nuking,*

el *ping* de la muerte y el *spoofing.* Ataques DdoS como *Smurf, stacheldraht y TFN,* son muy dañinos para las redes y los dispositivos de estas.

f. ***Capa de Enlace de Datos (Capa 2):*** Esta capa proporciona un tránsito fiable de datos por un enlace físico. Se encarga del direccionamiento físico, de la topología de la red, el acceso a la red, la notificación de errores, la entrega organizada de tramas y el control del flujo.

Entre los abusos y vulnerabilidades a nivel de trama están: el *sniffing,* el *spoofing,* tormentas de difusión y LAN virtuales (VLAN). Las NIC mal configuradas, causan problemas a segmentos de red o a la red entera.

g. ***Capa Física (Capa 1):*** Esta capa define las especificaciones eléctricas, mecánicas, procedimentales y funcionales para la activación, mantenimiento y desactivación del enlace físico entre los sistemas finales.

Esta capa es vulnerable a escuchas telefónicas y al reconocimiento. Los medios como el cobre y la fibra se pueden cortas por vándalos, ocasionando la caída de *hosts,* segmentos o redes enteras. Otros problemas son la inestabilidad eléctrica, por causas de desastres naturales, que pueden dejar inoperativos a los dispositivos.

1.4 AMENAZAS Y ATAQUES A LA SEGURIDAD INFORMÁTICA

1.4.1 Amenazas a las redes de datos. Hoy día, las amenazas a la red son más sofisticadas y requieren de menor conocimiento técnico para que un atacante realice su acción malintencionada contra la misma.

Las cuatro principales clases de amenazas para la seguridad de una red son las siguientes:

a. *Amenazas no estructuradas.* Constan principalmente de personas sin experiencia que emplean herramientas de pirateo, que se adquieren fácilmente (*Scripts Shell* y *Crackers* de contraseñas).

b. *Amenazas estructuradas.* Son las que representan los piratas altamente motivados y técnicamente competentes. Este tipo de personas conocen los puntos débiles del sistema, y pueden entender y desarrollar un código que los explote. Conocen, desarrollan y utilizan técnicas de pirateo sofisticadas para entrar en las organizaciones confiadas.

c. *Amenazas externas.* Son las amenazas provocadas por individuos o empresas que trabajan fuera de una empresa que no ha autorizado en acceso a los sistemas o redes de computadores. Estas personas laboran a través de Internet o de servidores de acceso por marcación telefónica.

d. *Amenazas internas.* Son las amenazas efectuadas dentro de la misma organización, cuando alguien ha autorizado el acceso a la red mediante una cuenta en un servidor o el acceso físico a la red.

1.4.2 Cuadro Sinóptico: Amenazas Informáticas

Figura 3. Diversas clasificaciones de las amenazas informáticas.

Fuente: PARRA CORRES, Carlos Alberto; Propuesta de diseño de un modelo de seguridad informática para la red de datos institucional de la Universidad Industrial de Santander [recurso electrónico] [ref. 18 Septiembre de 2006].

1.4.3 Ataques a las redes de datos. Con la existencia de numerosos puntos débiles y amenazas, la red queda expuesta gran cantidad y variedad de ataques.

Durante los primeros años de Internet, los ataques a sistemas informáticos requerían pocos conocimientos técnicos. Por un lado, los ataques realizados desde el interior de la red se basaban en la alteración de permisos para modificar la información del sistema. Por el contrario, los ataques externos se producían gracias al conocimiento de las contraseñas necesarias para acceder a los equipos de la red.

Con el paso de los años se han ido desarrollando nuevos ataques cada vez más sofisticados para explotar vulnerabilidades tanto en el diseño de las redes TCP/IP como en la configuración y operación de los sistemas informáticos que conforman las redes conectadas a Internet. Estos nuevos métodos de ataque se han ido automatizando, por lo que en muchos casos sólo se necesita un conocimiento técnico muy básico para realizarlos. Cualquier usuario con una conexión a Internet tiene acceso hoy en día a numerosas aplicaciones para realizar estos ataques y las instrucciones necesarias para ejecutarlos.

En la mayor parte de la bibliografía relacionada con la seguridad en redes informáticas se puede encontrar las tres generaciones de ataques clasificadas de la siguiente manera:

a. *Primera generación:* Ataques físicos. Aquí se encuentran los ataques que se centran en componentes electrónicos, como podrían ser los propios ordenadores, los cables o los dispositivos de red. Actualmente se conocen soluciones para estos ataques, utilizando protocolos distribuidos y de redundancia para conseguir una tolerancia a fallos aceptable.

b. *Segunda generación:* Ataques sintácticos. Se trata de ataques contra la lógica operativa de los computadores y las redes, que quieren explotar vulnerabilidades existentes en el software, algoritmos de cifrado y en protocolos. Aunque no existen soluciones globales para contrarrestar de forma eficiente estos ataques, se pueden encontrar soluciones cada vez más eficaces.

c. *Tercera generación:* Ataques semánticos. Finalmente, estos ataques se aprovechan de la confianza de los usuarios en la información. Este tipo de ataques pueden ir desde la colocación de información falsa en boletines informativos y correos electrónicos hasta la modificación del contenido de los datos en servicios de confianza, como, por ejemplo, la manipulación de bases de datos con información pública, sistemas de información bursátil, sistemas de control de tráfico aéreo, etc.

A continuación, después de conocer la clasificación de los tipos de ataques contra las redes de datos, se expondrán los ataques más comunes y frecuentes a las mismas, haciendo énfasis en la redes de las universidades más destacadas de Santander:

- **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.

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.

Los sniffers pueden ser una pesadilla para un administrador si son utilizados por usuarios no autorizados. Sin embargo, hay pocas herramientas tan poderosas como estas para detectar problemas en las redes. Es indispensable para un administrador de sistemas el conocer al menos el funcionamiento básico de estas herramientas y utilizarlas como parte de su rutina cotidiana.

- **Spam.** Se llama spam o correo basura a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en cantidades masivas que perjudican de una u otra manera al receptor. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es la basada en el correo electrónico.

  El spam no es un código dañino, pero si bastante molesto. Se trata de un programa que ejecuta una orden repetidas veces. Normalmente en el correo electrónico. Así un mensaje puede ser enviado varios cientos de veces a una misma dirección. En cualquier caso existen programas anti spam, ya que los spam son empleados normalmente por empresas de de publicidad directa.

El spam se puede difundir a través de diversos medios, entre ellos se destacan[4]:

a. *Spam por correo electrónico.* El correo electrónico es, con diferencia, el medio más común de spamming en Internet. Involucra enviar mensajes idénticos o casi idénticos a un gran número de direcciones. A diferencia de los correos electrónicos comerciales legítimos, el spam generalmente es enviado sin el permiso explícito de los receptores, y frecuentemente contiene varios trucos para sortear los filtros de spam. El receptor de spam puede verse perjudicado al tener que invertir tiempo en eliminar mensajes de su cuenta de correo electrónico.

b. *Spam por mensajería instantánea.* El spam por mensajería instantánea, también conocido como *spim*, utiliza los sistemas de mensajería instantánea, tales como ICQ o MSN Messenger. Muchos sistemas de mensajería ofrecen un directorio de usuarios, incluyendo información demográfica tal como edad y sexo. Los publicistas pueden reunir esta información, conectarse al sistema, y enviar mensajes no solicitados. Para enviar mensajes instantáneos a millones de usuarios de la mayoría de los servicios de mensajería instantánea sólo se requiere software de scripting y los nombres de usuario de los receptores.

c. *Spam en grupos de noticias.* El spam en grupos de noticias precede al spam por correo electrónico, y apunta a grupos de noticias Usenet. La antigua convención de Usenet define al spamming como publicación excesiva de múltiples mensajes, es decir, la publicación repetida de un mensaje (o mensajes sustancialmente similares). Debido a que publicar

[4] WIKIPEDIA, La enciclopedia libre. Spam [en línea]. [Fecha de consulta: 25 de septiembre de 2007]. Disponible en <http://es.wikipedia.org/w/index.php?title=Spam&oldid=12305593>.

mensajes en grupos de noticias es casi tan simple como enviar e-mails, los grupos de noticias son un objetivo popular para los spammers.

d. *Spam en foros.* El spam en un foro de Internet se produce cuando un usuario publica de manera reiterada una información o informaciones sustancialmente similares que desvirtúan o no tienen nada que ver con el tema de conversación.

- **Difusión de virus.** Un virus informático consiste en un programa que se copia automáticamente y que tiene por objeto alterar el normal funcionamiento de un computador, sin el permiso o el conocimiento del usuario.[5]

  La difusión de virus es si bien, un ataque de tipo tampering, y difiere de este porque puede ser ingresado al sistema por un dispositivo externo (diskettes – Discos Extraíbles) o través de la red (e-mail u otros protocolos) sin intervención directa del atacante.

  Existen distintos tipos de virus, como aquellos que infectan archivos ejecutables (.exe, .com, .bat, etc.) y los sectores de *boot-partition* de discos y diskettes, pero aquellos que causan en estos tiempos mas problemas son los macro-virus, que están ocultos en simples documentos o planillas 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.

  Entre las fases de infección de los virus se encuentran:

[5] WIKIPEDIA, La enciclopedia libre. Virus informático [en línea]. [Fecha de consulta: 25 de septiembre de 2007]. Disponible en <http://es.wikipedia.org/w/index.php?title=Virus_inform%C3%A1tico&oldid=12288392>.

a. *Fase de propagación o reproducción:* el virus hace copias de sí mismo en otros programas. Su funcionamiento es igual al de cualquier algoritmo de copia.

b. *Fase de activación o ataque:* el virus se activa para realizar la acción nociva para la cual fue diseñado. Al introducirse el virus, procederá a ocultarse para infectar archivos o esperar el momento de ejecutar su código de ataque, y con él sus rutinas dañinas. Este se puede alojar en el disco duro, bajo la apariencia de un archivo normal, sector de arranque, memoria principal, documentos con macros, entre otros.

c. *Fase de ejecución:* se ejecuta la función que puede ser inocua (mensaje en pantalla) o muy dañina (formatear un disco).

d. *Fase de defensa:* tiene como objetivo la protección del virus, el retardo en su detección, evitando todo aquello que provoque la remoción del virus. Es el módulo inteligente del virus.[6]

– **Caballos de troya[7].** Se denomina troyano o caballo de Troya, a un programa malicioso capaz de alojarse en computadores y permitir el acceso a usuarios externos, a través de una red local o de Internet, con el fin de recabar información o controlar remotamente a la máquina anfitriona.

Un troyano no es en sí, un virus, aún cuando teóricamente pueda ser distribuido y funcionar como tal. La diferencia fundamental entre un troyano y

[6] BARRAGÁN Ortiz, Luz Ángela. Análisis de desempeño de software de detección de Vulnerabilidades como herramienta para implementar estudio de Seguridad computacional en redes locales. Bucaramanga, 2004. Maestría en informática (Ingeniera de sistemas). Universidad Industrial de Santander. Facultad de ingenierías físico-mecánicas.

[7] WIKIPEDIA, La enciclopedia libre. Troyano (informática) [en línea]. [Fecha de consulta: 25 de septiembre de 2007]. Disponible en <http://es.wikipedia.org/w/index.php?title=Troyano_%28inform%C3%A1tica%29&oldid=12270830>

un virus consiste en su finalidad. Para que un programa sea un "troyano" solo tiene que acceder y controlar la máquina anfitriona sin ser advertido, normalmente bajo una apariencia inofensiva. Al contrario que un virus, que es un huésped destructivo, el troyano no necesariamente provoca daños porque no es su objetivo.

Suele ser un programa pequeño alojado dentro de una aplicación, una imagen, un archivo de música u otro elemento de apariencia inocente, que se instala en el sistema al ejecutar el archivo que lo contiene. Una vez instalado parece realizar una función útil (aunque cierto tipo de troyanos permanecen ocultos y por tal motivo los antivirus o anti-troyanos no los eliminan) pero internamente realiza otras tareas de las que el usuario no es consciente, de igual forma que el Caballo de Troya que los griegos regalaron a los troyanos.

Habitualmente se utiliza para espiar, usando la técnica para instalar un software de acceso remoto que permite monitorizar lo que el usuario legítimo de la computadora hace (en este caso el troyano es un spyware o programa espía) y, por ejemplo, capturar las pulsaciones del teclado con el fin de obtener contraseñas (cuando un troyano hace esto se le cataloga de keylogger) u otra información sensible.

La mejor defensa contra los troyanos es no ejecutar nada de lo cual se desconozca el origen y mantener software antivirus actualizado y dotado de buena heurística; es recomendable también instalar algún software anti troyano, de los cuales existen versiones gratis aunque muchas de ellas constituyen a su vez un troyano. Otra solución bastante eficaz contra los troyanos es tener instalado un firewall.

Otra manera de detectarlos es inspeccionando frecuentemente la lista de procesos activos en memoria en busca de elementos extraños, vigilar accesos a disco innecesarios, etc.

Lo peor de todo es que últimamente los troyanos están siendo diseñados de tal manera que es imposible poder detectarlos excepto por programas que a su vez contienen otro tipo de troyano, inclusive y aunque no confirmado, existen troyanos dentro de los programas para poder saber cual es el tipo de uso que se les da y poder sacar mejores herramientas al mercado llamados también "troyanos sociales".

Los troyanos están actualmente ilegalizados, pero hay muchos crackers que lo utilizan.

Los troyanos están compuestos principalmente por dos programas: un *cliente* (es quién envía las funciones que se deben realizar en la computadora infectada) y un *servidor* (recibe las funciones del cliente y las realiza, estando situado en la computadora infectada). También hay un archivo secundario llamado Librería (con la extensión *.dll) (pero que no todos los troyanos tienen de hecho los más peligrosos no lo tienen) que es necesaria para el funcionamiento del troyano pero no se debe abrir, modificar ni eliminar. Algunos troyanos también incluyen el llamado EditServer, que permite modificar el Servidor para que haga en el ordenador de la víctima lo que el cracker quiera.

Tipos de troyanos:

Los troyanos, a pesar de haber algunos ejemplos inofensivos, son casi siempre diseñados con propósitos dañinos. Se clasifican según:

a. La forma de penetración en los sistemas. Entre la forma de penetración a los sistemas se encuentran:

- Acceso remoto.
- Envío automático de e-mails.
- Destrucción de datos.
- Troyanos Proxy, que asumen ante otras computadoras la identidad de la infectada.
- Troyanos FTP (que añaden o copian datos de la computadora infectada).
- Deshabilitadores de programas de seguridad (antivirus, cortafuegos…).
- Ataque DoS a servidores (denial-of-service) hasta su bloqueo.
- Troyanos URL (Que conectan a la máquina infectada a través de conexiones de módem, normalmente de alto coste).

b. El daño que pueden causar. Entre los efectos que pueden producir a los sistemas atacados se encuentran:

- Borrar o sobrescribir datos en un equipo infectado.
- Cifrar archivos de la máquina, llevando al usuario al pago para recibir un código que le permita descifrarlos.
- Corromper archivos
- Descargar o subir archivos a la red.
- Permitir el acceso remoto al ordenador de la víctima. (Herramientas de administración remota o R.A.T)
- Reproducir otros programas maliciosos, como otros virus informáticos. En este caso se les denomina ‘droppers' o 'vectores'.
- Crear redes de ‘computadoras zombie’ infectadas para el lanzamiento de ataques de denegación de servicio contra servidores (DDoS) de

forma distribuida entre varios equipos o envío de correo no deseado (spam).

- Espiar y recolectar información sobre un usuario y enviar de incógnito los datos, como preferencias de navegación y estadísticas a otras personas
- Tomar capturas de pantalla en determinados momentos para saber lo que está viendo el usuario y así capaz detectar las contraseñas que se escriben en los teclados virtuales.
- Monitorizar las pulsaciones de teclas para robar información, nombres de usuario, contraseñas o números de tarjetas de crédito (keyloggers).
- Engañar al usuario mediante ingeniería social para conseguir sus datos y números bancarios y otros datos de su cuenta que pueden ser usados para propósitos delictivos.
- Instalación de puertas traseras en una computadora.
- Control de funciones físicas del equipo, como la apertura y cierre de los lectores de discos.
- Recolectar direcciones de correo electrónico y usarlas para enviar correo masivo o spam.
- Reiniciar el equipo cuando se ejecuta el programa.

– **Spoofing[8].** El spoofing hace referencia al uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación. Es usado para actuar en nombre de otros usuarios, a fin de realizar tareas de Snoofing o Tampering. Una forma común de spoofing, es conseguir el nombre y clave 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.

[8] WIKIPEDIA, La enciclopedia libre. Spoofing [en línea]. [Fecha de consulta: 25 de septiembre de 2007]. Disponible en <http://es.wikipedia.org/w/index.php?title=Spoofing&oldid=11963214>

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.

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.

Existen diferentes tipos de spoofing dependiendo de la tecnología a la que nos refiramos, los cuales se describirán más adelante, como el IP spoofing (quizás el más conocido), ARP spoofing, DNS spoofing, Web spoofing o e-mail spoofing, aunque en general se puede englobar dentro de spoofing cualquier tecnología de red susceptible de sufrir suplantaciones de identidad.

Tipos de Spoofing

a. *IP Spoofing.* Suplantación de IP. Consiste básicamente en sustituir la dirección IP origen de un paquete TCP/IP por otra dirección IP a la cual se desea suplantar. Esto se consigue generalmente gracias a programas destinados a ello y puede ser usado para cualquier protocolo dentro de TCP/IP como ICMP, UDP o TCP. Hay que tener en cuenta que las

respuestas del host que reciba los paquetes irán dirigidas a la IP falsificada. Por ejemplo si enviamos un ping (paquete icmp "echo request") spoofeado, la respuesta será recibida por el host al que pertenece la IP legalmente. Este tipo de spooofing unido al uso de peticiones broadcast a diferentes redes es usado en un tipo de ataque de flood conocido como smurf ataque. Para poder realizar IP SPOOFING en sesiones TCP, se debe tener en cuenta el comportamiento de dicho protocolo con el envío de paquetes SYN y ACK con su ISN específico y teniendo en cuenta que el propietario real de la IP podría (si no se le impide de alguna manera) cortar la conexión en cualquier momento al recibir paquetes sin haberlos solicitado. También hay que tener en cuenta que los routers actuales no admiten el envío de paquetes con IP origen no perteneciente a una de las redes que administra (los paquetes spoofeados no sobrepasarán el router).

b. *ARP Spoofing.* Suplantación de identidad por falsificación de tabla ARP. Se trata de la construcción de tramas de solicitud y respuesta ARP modificadas con el objetivo de falsear la tabla ARP (relación IP-MAC) de una víctima y forzarla a que envíe los paquetes a un host atacante en lugar de hacerlo a su destino legítimo. Explicándolo de una manera más sencilla: El protocolo Ethernet trabaja mediante direcciones MAC, no mediante direcciones IP. ARP es el protocolo encargado de traducir direcciones IP a direcciones MAC para que la comunicación pueda establecerse; para ello cuando un host quiere comunicarse con una IP emite una trama ARP-Request a la dirección de Broadcast pidiendo la MAC del host poseedor la IP con la que desea comunicarse. El ordenador con la IP solicitada responde con un ARP-Reply indicando su MAC. Los Switches y los hosts guardan una tabla local con la relación IP-MAC llamada "tabla ARP". Dicha tabla ARP puede ser falseada por un ordenador atacante que emita tramas ARP-REPLY indicando su MAC como destino válido para una IP específica, como por ejemplo la un router, de esta manera la información dirigida al router

pasaría por el ordenador atacante quien podrá sniffear dicha información y redirigirla si así lo desea. El protocolo ARP trabaja a nivel de enlace de datos de OSI, por lo que esta técnica solo puede ser utilizada en redes LAN o en cualquier caso en la parte de la red que queda antes del primer Router. La manera más sencilla de protegerse de esta técnica es mediante tablas ARP estáticas (siempre que las IPs de red sean fijas).

c. *DNS Spoofing.* Suplantación de identidad por nombre de dominio. Se trata del falseamiento de una relación "Nombre de dominio-IP" ante una consulta de resolución de nombre, es decir, resolver con una dirección IP falsa un cierto nombre DNS o viceversa. Esto se consigue falseando las entradas de la relación Nombre de dominio-IP de un servidor DNS, mediante alguna vulnerabilidad del servidor en concreto o por su confianza hacia servidores poco fiables. Las entradas falseadas de un servidor DNS son susceptibles de infectar (envenenar) el caché DNS de otro servidor diferente (DNS Poisoning).

d. *Web Spoofing.* Suplantación de una página Web real (no confundir con phising). Enruta la conexión de una víctima a través de una página falsa hacia otras páginas WEB con el objetivo de obtener información de dicha víctima (páginas WEB visitas, información de formularios, contraseñas etc.). La página WEB falsa actúa a modo de Proxy solicitando la información requerida por la víctima a cada servidor original y saltándose incluso la protección SSL. El atacante puede modificar cualquier información desde y hacia cualquier servidor que la víctima visite. La víctima puede abrir la página Web falsa mediante cualquier tipo de engaño, incluso abriendo un simple LINK. El WEB SPOOFING es difícilmente detectable, quizá la mejor medida es algún plugin del navegador que muestre en todo momento la IP del servidor visitado, si la IP nunca cambia al visitar diferentes páginas WEB significará que probablemente estemos sufriendo este tipo de ataque.

e. *Mail Spoofing***.** Suplantación en correo electrónico de la dirección e-mail de otras personas o entidades. Esta técnica es usada con asiduidad para el envío de e-mails hoax como suplemento perfecto para el uso de phising y para SPAM, es tan sencilla como el uso de un servidor SMTP configurado para tal fin. Para protegerse se debería comprobar la IP del remitente (para averiguar si realmente esa IP pertenece a la entidad que indica en el mensaje) y la dirección del servidor SMTP utilizado. Otra técnica de protección es el uso de firmas digitales.

- **Obtención de passwords, códigos y claves[9].** 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 la contraseña correcta.

- **Bombas lógicas[10].** Es un programa informático que se instala en un computador y permanece oculto hasta cumplirse una o más condiciones preprogramadas para entonces ejecutar una acción. Este suele ser el procedimiento de sabotaje que comúnmente usan empleados descontentos.

  Una bomba lógica tiene por objeto introducir un programa o rutina que bajo condiciones predeterminadas tales como: un día de la semana concreto, una hora concreta, la pulsación de una tecla o una secuencia de teclas concreta o

[9] BARRAGÁN Op. cit., p 58
[10] WIKIPEDIA, La enciclopedia libre. Bomba lógica [en línea]. [Fecha de consulta: 26 de septiembre de 2007]. Disponible en <http://es.wikipedia.org/w/index.php?title=Bomba_l%C3%B3gica&oldid=12350797>

la ejecución de un archivo concreto, ejecuta acciones como: Borrar la información del disco duro, Mostrar un mensaje, Reproducir una canción o Enviar un correo electrónico.

- **Ingeniera social.** Básicamente es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Convencer a la gente de que haga lo que en realidad no debería.[11]

  Un ingeniero social usará comúnmente el teléfono o Internet para engañar a la gente y llevarla a revelar información sensible, o bien a violar las políticas de seguridad típicas. Con este método, los ingenieros sociales aprovechan la tendencia natural de la gente a confiar en su palabra, antes que aprovechar agujeros de seguridad en los sistemas informáticos. Generalmente se está de acuerdo en que "los usuarios son el eslabón débil" en seguridad; éste es el principio por el que se rige la ingeniería social.

  Un ejemplo clásico de Ingeniería Social sería llamar a un usuario haciéndose pasar por administrador del sistema y requerirle la contraseña con alguna excusa convincente. Esto es común cuando en el Centro de Cómputo los administradores son amigos o conocidos.

- **Gusanos informáticos[12].** Un gusano es un virus informático que tiene la propiedad de duplicarse a sí mismo. Los gusanos utilizan las partes automáticas de un sistema operativo que generalmente son invisibles al usuario.

[11] BARRAGÁN Op. Cit., p 58

[12] WIKIPEDIA, La enciclopedia libre. Gusano informático [en línea]. [Fecha de consulta: 25 de septiembre de 2007]. Disponible en <http://es.wikipedia.org/w/index.php?title=Gusano_inform%C3%A1tico&oldid=12148416>

A diferencia de un virus, un gusano no precisa alterar los archivos de programas, sino que reside en la memoria y se duplica a sí mismo. Los gusanos siempre dañan la red (aunque sea simplemente consumiendo ancho de banda), mientras que los virus siempre infectan o corrompen los archivos de la computadora que atacan.

Es algo usual detectar la presencia de gusanos en un sistema cuando, debido a su incontrolada replicación, los recursos del sistema se consumen hasta el punto de que las tareas ordinarias del mismo son excesivamente lentas o simplemente no pueden ejecutarse.

Los gusanos se basan en una red de computadoras para enviar copias de sí mismo a otros nodos (es decir, a otras terminales en la red) y es capaz de llevar esto a cabo sin intervención del usuario.

Después de haber realizado una recopilación bibliográfica y un estudio preliminar sobre los ataques más frecuentes que sufren las redes, a continuación se expone la tabulación de una encuesta realizada a las principales instituciones universitarias de Santander sobre aspectos relevantes referente al nivel de seguridad implementado en su (s) red (es) institucional (es).

- **Snooping y downloading[13].** Estos ataques tienen el mismo objetivo que el sniffing, obtener la información sin alterarla. 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 una descarga de esa información a su propia computadora.

[13] BARRAGÁN Op. Cit., p. 58.

- **Tampering o data diddling[14].** Este ataque 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 comprobar y tratar de recuperar aquella información que ha sido alterada o borrada.

- **Jamming o flooding[15].** 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.

- **Explotación de errores de diseño, implementación u operación[16].** 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.

[14] Ibid., p. 58.
[15] Ibid., p. 58.
[16] Ibid., p. 58.

- **Eliminar el blanco. Ping mortal[17].** 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 quede sin recursos y se “cuelgue”.

- **Land attack[18].** Es otro método empleado para “colgar” un equipo es. Este ataque 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.

- **Supernuke[19].** Es un ataque característico de los equipos con Windows como sistema operativo. Supernuke es también llamado Winnuke. Este ataque hace que los equipos que escuchan por el puerto UDP 139 se “cuelguen”.

1.5 TÉCNICAS PARA LA SEGURIDAD INFORMÁTICA

1.5.1 Sistema de detección de intrusos (IDS). El aumento y la gravedad de los ataques hoy en día hacen que los sistemas de detección de intrusos sean una parte indispensable de la seguridad informática en cualquier sistema de información.

Las empresas tienen buenas razones comerciales y legales para establecer sólidas políticas de seguridad. Después de todo, su existencia depende de dichas políticas. Sin embargo, la empresa que no controle el abuso de estas políticas perderá un importante componente de seguridad. Si no implementan ningún

[17] Ibid., p. 58.
[18] Ibid., p. 58.
[19] Ibid., p. 58.

control, los ejecutivos nunca sabrán si se cumplen sus políticas de seguridad. Por esta razón, es esencial instalar un Sistema de Detección de Intrusos (IDS).

A continuación se muestra que es un IDS, su funcionamiento y los tipos de IDS que existen, entre otros aspectos más a tratar.

- **¿Qué es un sistema de detección de intrusos?** Un sistema de detección de intrusos es un programa activo que analiza la actividad del sistema y de la red para detectar accesos desautorizados y/o actividades maliciosas sobren un computador o sobre una red. Estos accesos pueden ser ataques de habilidosos hackers, o de Script Kiddies que usan herramientas automáticas.

  La forma en que un IDS detecta las anomalías pueden variar ampliamente; sin embargo, el objetivo final de cualquier IDS es el de atrapar a los perpetradores en el acto antes de que hagan algún daño a sus recursos. 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.

  Un IDS protege a un sistema contra ataques, malos usos y compromisos. Puede también monitorear la actividad de la red, auditar las configuraciones de la red y sistemas por vulnerabilidades, analizar la integridad de los datos y más. Dependiendo de los métodos de detección que seleccione utilizar, existen numerosos beneficios directos e incidentales de usar un IDS.

- **¿Cómo funciona un sistema de detección de intrusos?**[20] El funcionamiento de estas herramientas se basa en el análisis detallado 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.

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

  Los IDS suelen disponer de una base de datos de “firmas” de ataques conocidos.

  Dichas firmas permiten al IDS distinguir entre el uso normal del PC y el uso fraudulento, y/o entre el tráfico normal de la red y el tráfico que puede ser resultado de un ataque o intento del mismo.

- **Tipos de sistemas de detección de intrusos.** Entender que es un IDS y las funciones que proporciona, es clave para determinar cuál será el tipo apropiado para incluir en una política de seguridad de una empresa u organización.

[20] WIKIPEDIA, La enciclopedia libre. Sistema de detección de intrusos [en línea]. [Fecha de consulta: 26 de septiembre de 2007]. Disponible en <http://es.wikipedia.org/w/index.php?title=Sistema_de_detecci%C3%B3n_de_intrusos&oldid=11187021>

Algunos IDSes están basados en *conocimiento*, lo que alerta a los administradores de seguridad antes de que ocurra una intrusión usando una base de datos de ataques comunes. Alternativamente, existen los IDS basados en *comportamiento*, que hacen un seguimiento de todos los recursos usados buscando cualquier anomalía, lo que es usualmente una señal positiva de actividad maliciosa.

Los tipos más importantes de IDSes mencionados en el campo de seguridad son conocidos como IDSes basados en host, basados en red y basados en una arquitectura Cliente-Servidor. Un IDS basado en host es el más completo de los dos, que implica la implementación de un sistema de detección en cada host individual. Sin importar en qué ambiente de red resida el host, estará protegido. Un IDS basado en la red filtra los paquetes a través de un dispositivo simple antes de comenzar a enviar a host específicos. Los IDSes basados en red a menudo se consideran como menos completos puestos que muchos host en un ambiente móvil lo hacen indisponible para el escaneo y protección de paquetes de red. Y finalmente un IDS basado en la arquitectura cliente-servidor, esta compuesto por una serie de IDSes de red 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 IDS de red se puede fijar unas reglas de control especializándose para cada segmento de red. Es la estructura habitual en redes privadas virtuales (VPN).

a. *IDS basados en Host (HIDS – HostIDS)*[21]. Un IDS basado en host analiza diferentes áreas para determinar el uso incorrecto (actividades maliciosas o abusivas dentro de la red) o alguna intrusión (violaciones desde afuera). Los IDSes basados en host consultan diferentes tipos de registros de

[21] Red Hat, Inc. Red Hat Enterprise Linux 4: Manual de seguridad. IDS basados en host. [en línea]. [Fecha de consulta: 26 de septiembre de 2007]. Disponible en <http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/s1-ids-host.html>

archivos (kernel, sistema, servidores, red, cortafuegos, y más) y comparan los registros contra una base de datos interna de singularidades comunes sobre ataques conocidos.

Los IDSes basados en hosts filtran los registros (lo cual, en el caso de algunas redes y registros de eventos del kernel pueden ser bastante detallados), los analizan, vuelven a etiquetar los mensajes anómalos con su propia clasificación de severidad y los reúne en su propio registro para que sean analizados por el administrador.

Los IDSes basados en host también pueden verificar la integridad de los datos de archivos y ejecutables importantes. Funciona verificando una base de datos de archivos confidenciales (y cualquier archivo añadido por el administrador) y crea una *suma de verificación* de cada archivo con una utilidad de resumen de archivos de mensajes tal como md5sum (algoritmo de 128-bit) o sha1sum (algoritmo de 160-bit). El IDS basado en host luego almacena las sumas en un archivo de texto plano y periódicamente compara las sumas de verificación contra los valores en el archivo de texto. Si cualquiera de estas sumas no coinciden, el IDS alertará al administrador a través de un correo electrónico o a un mensaje al celular.

b. *IDS basados en Red (NIDS - NetworkIDS)*[22]. Los sistemas de detección de intrusos basados en la red operan de una forma diferente que aquellos IDSes basados en host. La filosofía de diseño de un IDS basado en la red es escanear los paquetes de red al nivel del router o host, auditar la información de los paquetes y registrar cualquier paquete sospechoso en un archivo de registros especial con información extendida. Basándose en estos paquetes sospechosos, un IDS basado en la red puede escanear su

[22] Red Hat, Inc. Red Hat Enterprise Linux 4: Manual de seguridad. IDS basados en la red. [en línea]. [Fecha de consulta: 26 de septiembre de 2007]. Disponible en <http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/s1-ids-net.html>

propia base de datos de firmas de ataques a la red y asignarles un nivel de severidad para cada paquete. Si los niveles de severidad son lo suficientemente altos, se enviará un correo electrónico o un mensaje de pager de advertencia a los miembros del equipo de seguridad para que ellos puedan investigar la naturaleza de la anomalía.

Los IDSes basados en la red se han vuelto muy populares a medida en que la Internet ha crecido en tamaño y tráfico. Los IDSes que son capaces de escanear grandes volúmenes de actividad en la red y exitosamente etiquetar transmisiones sospechosas, son bien recibidos dentro de la industria de seguridad. Debido a la inseguridad inherente de los protocolos TCP/IP, se ha vuelto imperativo desarrollar escaners, husmeadores y otras herramientas de auditoria y detección para así prevenir violaciones de seguridad por actividades maliciosas en la red, tales como:

- Engaño de direcciones IP (IP Spoofing)
- Ataques de rechazo de servicio (DoS)
- Envenenamiento de caché ARP.
- Corrupción de nombres DNS
- Ataques de hombre en el medio

c. *IDS basados en Arquitectura Cliente-Servidor (DIDS - DistributedIDS)*[23]. 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

[23] WIKIPEDIA Op. Cit., p. 72.

especializándose para cada segmento de red. Es la estructura habitual en redes privadas virtuales (VPN).

- **Sistemas de detección de intrusos pasivos y sistemas reactivos[24]**

  a. *IDSes Pasivos:* Son aquellos IDS que notifican a la autoridad competente o administrador de la red mediante el sistema que sea, alerta, etc. El sensor detecta una posible intrusión, almacena la información y manda una señal de alerta que se almacena en una base de datos, pero no actúa sobre el ataque o atacante.

  b. *IDSes Reactivos:* Generan algún tipo de respuesta sobre el sistema atacante o fuente de ataque como cerrar la conexión o enviar algún tipo de respuesta predefinida en nuestra configuración.

- **Implementación de un IDS[25].** Para colocar en funcionamiento un sistema de detección de intrusos se debe tener en cuenta que es posible optar por una solución hardware, software o incluso una combinación de estos dos.

  Algunos aspectos a tener en cuenta en el momento de implementar un IDS son:

  a. *Respuesta*: Un Sistema de detección de intrusos IDS debe ir más allá de la simple notificación proporcionando respuestas automatizadas basadas en políticas para proteger los sistemas y ofreciendo tiempo y tranquilidad al personal de seguridad. Cuando es necesario localizar el origen de un ataque (frecuentemente se ataca con una dirección falsificada), el enfoque

[24] Ibid., p. 72.
[25] INTERLAN. Ingeniería de redes y sistemas LTDA. Evaluación de los Sistemas de Detección de Intrusos (IDS). Publicado el 30 de Septiembre del 2003. [en línea]. [Fecha de consulta: 26 de septiembre de 2007]. Disponible en <http://www.interlan.com.co/ids.htm >

tradicional ha sido interrogar manualmente a los routers y encontrar el flujo relevante de los datos. Este es un ejercicio agotador que puede llevar muchas horas o días, incluso para un ingeniero de redes experimentado. Una empresa debe a cambio escoger un IDS que pueda rastrear los ataques rápida y automáticamente, incluso aquellos que son falsificados o que se reflejan, de regreso al punto de ingreso de la red. Esto permitirá a la empresa reaccionar rápida y eficientemente para bloquear los ataques de negación de servicio que pueden afectar la disponibilidad del ancho de banda y del servicio.

b. *Instalación:* Un sistema IDS debería poder manejar los escenarios de instalación más grandes y exigentes, incluso el monitoreo de los múltiples segmentos de la red. También debería ser capaz de proteger las infraestructuras de la información empresarial mediante la detección de múltiples gigabits de alta velocidad.

c. *Análisis:* Un sistema IDS debería tener un motor de análisis y correlación que analizase los numerosos eventos que suceden en la red y los evaluase en contexto. El tiempo y el conocimiento son críticos para lanzar una respuesta rápida y efectiva a los ataques contra los activos empresariales de misión crítica en el momento en que se produzcan. La acumulación de eventos en tiempo real, la correlación y el análisis pueden reducir dramáticamente el esfuerzo que tradicionalmente se exige del personal de seguridad para darle tiempo a que realice un trabajo investigativo sobre los sofisticados intrusos y las políticas en lugar de pasar horas examinando los registros de eventos no correlacionados.

d. *Facilidad de administración:* Un sistema IDS debe recoger los datos importantes de detección directamente de los conmutadores de redes, lo

que reduce la cantidad de sensores que se necesita instalar y administrar en toda la red a fin de reducir el Costo Total de Propiedad (TCO).

e. *Costo de expansión:* Muchas empresas no se dan cuenta de que la ampliación de los sistemas IDS diseñados específicamente para redes conmutadas de alta velocidad cuestan menos que la de los sistemas tradicionales. Una instalación tradicional requiere de un sensor para cada segmento de la red, además del costo del hardware, software y de la administración del sistema. Cuando una compañía necesita expandirse para tener cobertura de red total, los costos asociados al financiamiento de los sensores, hardware, software y administración del sistema serán comparables a los costos de aquellos componentes de la instalación inicial. Por el contrario, un sistema IDS diseñado para funcionar en redes conmutadas de alta velocidad permite una cobertura máxima sin el costo agregado de la administración del sistema. Un sistema IDS con la herramienta de localización puede compararse a un grupo de cámaras de seguridad almacenadas convenientemente. Sin embargo, a diferencia de las cámaras de seguridad, el sistema IDS debe tener la inteligencia para saber que ha ocurrido un incidente, para continuar recogiendo datos y alertar al administrador del sistema. Con este tipo de sistema IDS, los ahorros empresariales sólo en concepto de soporte, instalación y mantenimiento pueden ser significativos.

- **Firewalls.** Actualmente Internet se ha convertido en una herramienta imprescindible de comunicación para las organizaciones. La puerta de acceso a esta Red por donde circula la información es un camino de doble sentido y esto trae como consecuencia unos mayores riesgos para la seguridad de las redes empresariales, gubernamentales y privadas. Es en este punto donde el valor de los contrafuegos toma sentido en el momento de su implementación

en diversas redes de datos, pues es considerado como un sistema básico de seguridad que debería instalarse para conectarse a la red de redes, Internet.

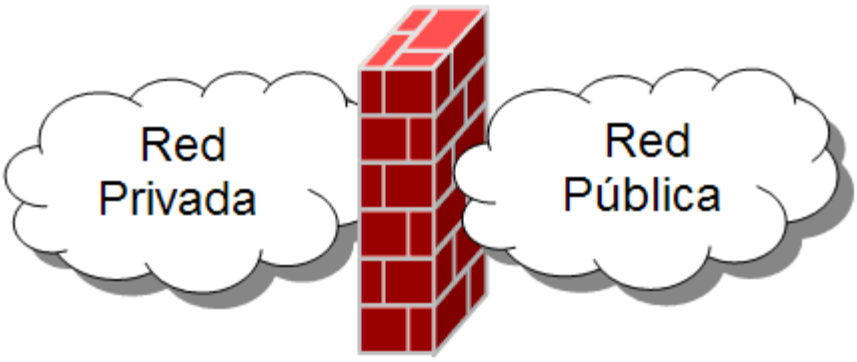
Un contrafuego o Firewall, es un elemento de hardware o software empleado en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de seguridad que hayan sido definidas por la organización responsable de la red.

En otros términos, un firewall es un sistema de defensa que se basa en la instalación de una "barrera" entre el PC y la Red, por la que circulan todos los datos. Este tráfico entre la Red y el PC es autorizado o denegado por el firewall (la "barrera"), siguiendo las instrucciones que se le hayan configurado.

Su manera de funcionar es indicada en el RFC 2979, que define las características de comportamiento y requerimientos de interoperabilidad.

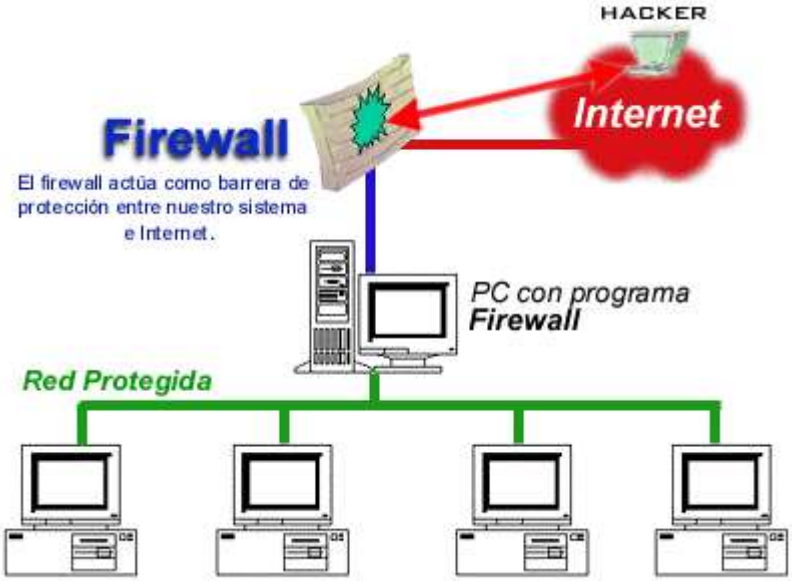
La ubicación habitual de un cortafuegos es el punto de conexión de la red interna de la organización con la red exterior, que normalmente es Internet; de este modo se protege la red interna de intentos de acceso no autorizados desde Internet, que puedan aprovechar vulnerabilidades de los sistemas de la red interna. Ver Figura No. 4 y Figura No. 5

Figura 4. Ubicación Estratégica de Un Firewall.



Fuente: (Traducido y adaptado de) Wikipedia, La enciclopedia libre, *Cortafuegos (informática)* [en línea]. [Fecha de consulta: 12 de marzo del 2007]. Disponible en: <http://es.wikipedia.org/wiki/Cortafuegos_%28inform%C3%A1tica%29>

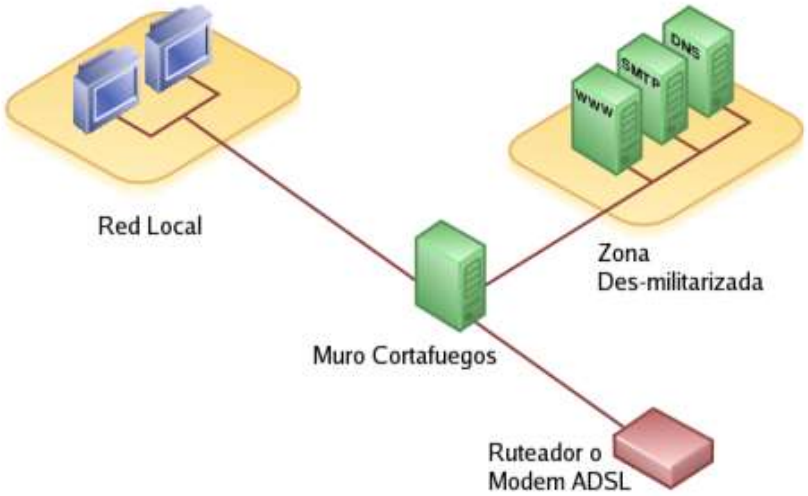
Figura 5. Ejemplo Clásico De Un Firewall En Una Red De Datos



Fuente: InfoSpyware, Seguridad en la red [en línea]. [Fecha de consulta: 12 de marzo de 2007]. Disponible en: http://www.infospyware.com/Firewall/Cortafuegos.htm

También es frecuente conectar al cortafuego una tercera red, llamada zona desmilitarizada o DMZ, en la que se ubican los servidores (como servidores de e-mail, Web y DNS) de la organización que deben permanecer accesibles desde la red exterior. Ver Figura No. 6.

Figura 6. Zona Desmilitarizada (DMZ) o Red Perimetral



Fuente: Barrios Dueñas, Joel, Configurar un muro cortafuegos. [en línea]. [Fecha de consulta: 12 de marzo de 2007]. Disponible en: http://www.linuxparatodos.net/portal/staticpages/index.php?page=como-shorewall-3-interfaces-red

Un cortafuego correctamente configurado añade protección a una instalación informática, pero en ningún caso debe considerarse como suficiente. La Seguridad informática abarca más ámbitos y más niveles de trabajo y protección.

- **Tipos de Firewall**

a. *Cortafuegos de capa de red o de filtrado de paquetes.* Funciona a nivel de red (capa 3) de la pila de protocolos (TCP/IP) como filtro de paquetes IP. A este nivel el router puede realizar filtros según los distintos campos de los paquetes IP: dirección IP origen, dirección IP destino. A menudo en este tipo de cortafuegos se permiten filtrados según campos de nivel de transporte (capa 4) como el puerto origen y destino, o a nivel de enlace de datos (capa 2) como la dirección MAC.

   Este tipo de contrafuegos tienen la ventaja de ser económicos, de tener un alto nivel de desempeño y de ser transparentes para los usuarios conectados a la red. Sin embargo presenta debilidades como:

   - No protege las capas superiores a nivel OSI.
   - Las necesidades aplicativas son difíciles de traducir como filtros de protocolos y puertos.
   - No son capaces de esconder la topología de redes privadas, por lo que exponen la red al mundo exterior.
   - Sus capacidades de auditoria suelen ser limitadas, al igual que su capacidad de registro de actividades.
   - No soportan políticas de seguridad complejas como autentificación de usuarios y control de accesos con horarios prefijados.

b. *Cortafuegos de capa de aplicación.* Trabaja en el nivel de aplicación (capa 7) 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. Un cortafuego a nivel 7 de tráfico HTTP es normalmente denominado Proxy

y permite que los computadores de una organización entren a Internet de una forma controlada.

c. *Cortafuego personal.* Es un caso particular de cortafuegos que se instala como software en un computador, filtrando las comunicaciones entre dicho computador y el resto de la red y viceversa.

- **Ventajas de un Firewall**

a. *Protege de intrusiones.* 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.

b. *Protección de información privada.* 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 la información que le son estrictamente necesarios.

c. *Optimización de acceso.* Identifica los elementos de la red internos y optimiza que la comunicación entre ellos sea más directa. Esto ayuda a reconfigurar los parámetros de seguridad.

- **Limitaciones de un Firewall**

a. Un firewall no puede protegerse contra aquellos ataques que se efectúen fuera de su punto de operación.

b. El cortafuegos no puede protegerse de las amenazas a que esta sometido por atacantes o usuarios inconscientes. El firewall no puede prohibir que los

traidores o espías corporativos copien datos sensibles en disquetes o tarjetas PCMCIA y sustraigan éstas del edificio.

c. El firewall no puede proteger contra los ataques de Ingeniería social.

d. El firewall no puede protegerse contra los ataques posibles a la red interna por virus informáticos a través de archivos y software. La solución real esta en que la organización debe ser consciente en instalar software antivirus en cada máquina para protegerse de los virus que llegan por medio de disquetes o cualquier otra fuente.

e. El firewall no protege de los fallos de seguridad de los servicios y protocolos de los cuales se permita el tráfico. Hay que configurar correctamente y cuidar la seguridad de los servicios que se publiquen a Internet.

- **Políticas de los Firewalls**

Hay dos políticas básicas en la configuración de un firewall que cambian radicalmente la filosofía fundamental de la seguridad en la organización:

a. *Política restrictiva:* Se deniega todo el tráfico excepto el que está explícitamente permitido. El firewall obstruye todo el tráfico y hay que habilitar expresamente el tráfico de los servicios que se necesiten.

b. *Política permisiva:* Se permite todo el tráfico excepto el que esté explícitamente denegado. Cada servicio potencialmente peligroso necesitará ser aislado básicamente caso por caso, mientras que el resto del tráfico no será filtrado.

La política restrictiva es la más segura, ya que es más difícil permitir por error tráfico potencialmente peligroso, mientras que en la política permisiva es posible que no se haya contemplado algún caso de tráfico peligroso y sea permitido por defecto.

1.5.2 Antivirus. Los antivirus son programas cuya función es detectar y eliminar Virus informáticos y otros programas maliciosos *(a veces denominados malware).*

Básicamente, un antivirus compara el código de cada archivo con una base de datos de los códigos (también conocidos como firmas o vacunas) de los virus conocidos, por lo que es importante actualizarla periódicamente a fin de evitar que un virus nuevo no sea detectado. También se les ha agregado funciones avanzadas, como la búsqueda de comportamientos típicos de virus (técnica conocida como Heurística) o la verificación contra virus en redes de computadoras.

Normalmente un antivirus tiene un componente que se carga en memoria y permanece en ella para verificar todos los archivos abiertos, creados, modificados y ejecutados en tiempo real. Es muy común que tengan componentes que revisen los adjuntos de los correos electrónicos salientes y entrantes, así como los scripts y programas que pueden ejecutarse en un navegador Web (ActiveX, Java, JavaScript).

Los virus, gusanos, spyware, entre otros, son programas informáticos que se ejecutan normalmente sin el consentimiento del legítimo del propietario y que tienen la característica de ejecutar recursos, consumir memoria e incluso eliminar o destrozar la información. Una característica adicional es la capacidad que tienen de propagarse. Otras características son el robo de información, la pérdida de

esta, la capacidad de suplantación, que hacen que reviertan en pérdidas económicas y de imagen.

Los antivirus tratan de descubrir las trazas que ha dejado un software malicioso, para eliminarlo o detectarlo, y en algunos casos contener o parar la contaminación.

Los métodos para contener o reducir los riesgos asociados a los virus pueden ser los denominados activos o pasivos.

a. *Antivirus (activo).* Estos programas tratan de encontrar la traza de los programas maliciosos mientras el sistema esta en funcionamiento.

   Así mismo, tratan de tener controlado el sistema mientras funciona parando las vías conocidas de infección y notificando al usuario de posibles incidencias de seguridad.

   Como programa que esté continuamente funcionando, el antivirus tiene un efecto adverso sobre el sistema en funcionamiento. Una parte importante de los recursos se destinan al funcionamiento del mismo. Además dado que están continuamente comprobando la memoria de la máquina, dar más memoria al sistema no mejora las prestaciones del mismo.

   Otro efecto adverso son los falsos positivos, es decir al notificar al usuario de posibles incidencias en la seguridad, éste que normalmente no es un experto de seguridad se acostumbra a dar al botón de autorizar a todas las acciones que le notifica el sistema. De esta forma el antivirus funcionando da una sensación de falsa seguridad.[26]

[26] WIKIPEDIA, La enciclopedia libre. Antivirus [en línea]. [Fecha de consulta: 27 de septiembre de 2007]. Disponible en <http://es.wikipedia.org/w/index.php?title=Antivirus&oldid=12357804>

Un antivirus tiene tres principales funciones y componentes principales:

I. Vacuna: Es un programa que instalado residente en la memoria, actúa como "filtro" de los programas que son ejecutados, abiertos para ser leídos o copiados, en tiempo real**.**

II. Detector: Es el programa que examina todos los archivos existentes en el disco o a los que se les indique en una determinada ruta o PATH. Tiene instrucciones de control y reconocimiento exacto de los códigos virales que permiten capturar sus pares, debidamente registrados y en forma sumamente rápida desarman su estructura.

III. Eliminador: Es el programa que una vez desactivada la estructura del virus procede a eliminarlo e inmediatamente después a reparar o reconstruir los archivos y áreas afectadas.

b. *Filtros de archivos (activo).* Otra aproximación es la de generar filtros dentro de la red que proporcionen un filtrado más selectivo. Desde el sistema de correos, hasta el empleo de técnicas de firewall, proporcionan un método activo y eficaz de eliminar estos contenidos.

   En general este sistema proporciona una seguridad donde el usuario no requiere de intervención, puede ser más tajante, y permitir emplear únicamente recursos de forma más selectiva.

   Cuando el número de puestos a filtrar crece puede ser conveniente.

c. Copias de seguridad (pasivo). Mantener una política de copias de seguridad garantiza la recuperación de los datos y la respuesta cuando nada de lo anterior ha funcionado.

Asimismo las empresas deberían disponer de un plan y detalle de todo el software instalado para tener un plan de contingencia en caso de problemas.

1.5.3 Proxies. 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. Sin 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.).

Entre las ventajas de los Proxies se encuentran:

a. *Control*. Sólo el intermediario hace el trabajo real, por tanto se pueden limitar y restringir los derechos de los usuarios, y dar permisos sólo al Proxy.

b. *Ahorro*. Por tanto, sólo *uno* de los usuarios (el proxy) ha de estar equipado para hacer el trabajo real.

c. *Velocidad*. Si varios clientes van a pedir el mismo recurso, el proxy puede hacer caché: guardar la respuesta de una petición para darla directamente cuando otro usuario la pida. Así no tiene que volver a contactar con el destino, y acaba más rápido.

d. *Filtrado*. El proxy puede negarse a responder algunas peticiones si detecta que están prohibidas.

e. *Modificación*. Como intermediario que es, un proxy puede falsificar información, o modificarla siguiendo un algoritmo.

f. *Anonimato.* Si todos los usuarios se identifican como uno sólo, es difícil que el recurso accedido pueda diferenciarlos. Pero esto puede ser malo, por ejemplo cuando hay que hacer necesariamente la identificación.

1.5.4 Wrappers[27]. El gran desarrollo que han tenido las redes de computadoras han abierto a los usuarios posibilidades nunca antes imaginadas. Actualmente una persona puede tener acceso a información que está físicamente localizada del otro lado del Planeta, o comunicarse en cuestión de segundos con personas ubicadas a muchos kilómetros de distancia.

[27] WIKIPEDIA, La enciclopedia libre. TCP Wrapper [en línea]. [Fecha de consulta: 27 de septiembre de 2007].Disponible en <http://es.wikipedia.org/w/index.php?title=TCP_Wrapper&oldid=12360698>

Esto ha cambiado la forma como muchos de nosotros vemos y usamos a las computadoras. Sin embargo también ha abierto la posibilidad a muchos problemas. A través de los mismos servicios de red que nos permiten difundir y obtener información, en muchas ocasiones ha sido posible obtener acceso no autorizado a los sistemas, permitiendo a los intrusos utilizar recursos a los que no deberían tener acceso, o incluso realizar actos dañinos como robar o destruir información.

Los requerimientos de la seguridad varían dependiendo de la complejidad de las tareas o actividades en las cuales se emplea el equipo de cómputo y de la plataforma de equipo que éstas involucren. Las medidas de seguridad necesarias para proteger una PC no es la misma que las medidas de seguridad necesarias para garantizar el funcionamiento continuo de una red de área local (LAN), y éstas a su vez son menores a las requeridas cuando se trata de una de red área amplia (WAN), que sería el caso de la conexión a INTERNET.

TCP Wrappers permite controlar y proteger los servicios de red, limitando el acceso como sea posible, y registrado todos las conexiones para hacer el trabajo de detectar y resolver problemas de forma más fácil.

TCP Wrappers es una herramienta simple que sirve para monitorear y controlar el tráfico que llega por la red. Esta herramienta ha sido utilizada exitosamente en la protección de sistemas y la detección de actividades ilícitas. Fue desarrollada por Wietze Zweitze Venema y esta basada en el concepto de Wrapper; es una herramienta de seguridad libre y muy útil.

Un Wrapper es un programa para controlar el acceso a un segundo programa. El Wrapper literalmente cubre la identidad del segundo programa, obteniendo con esto un más alto nivel de seguridad.

Los Wrappers son usados dentro de la Seguridad en Sistemas UNIX. Estos programas nacieron de 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:

a. Debido a que la seguridad lógica esta concentrada en un solo programa, los Wrappers son fáciles y simples de validar.

b. Debido a que el programa protegido se mantiene como una entidad separada, éste puede ser actualizado sin necesidad de cambiar el Wrapper.

c. Debido a que los Wrappers llaman al programa protegido mediante la llamada al sistema estándar exec(), se puede usar un solo Wrapper para controlar el acceso a diversos programas que se necesiten proteger.

1.5.5 Criptografía. La criptografía (del griego *kryptos*, «ocultar», y *graphos*, «escribir», literalmente «escritura oculta») es el arte o ciencia de cifrar y descifrar información utilizando técnicas matemáticas que hagan posible el intercambio de mensajes de manera que sólo puedan ser leídos por las personas a quienes van dirigidos.

La finalidad de la criptografía es, en primer lugar, garantizar el secreto en la comunicación entre dos entidades (personas, organizaciones, etc.) y, en segundo lugar, asegurar que la información que se envía es auténtica en un doble sentido: que el remitente sea realmente quien dice ser y que el contenido del mensaje enviado, habitualmente denominado criptograma, no haya sido modificado en su tránsito.

En la actualidad, la criptografía no sólo se utiliza para comunicar información de forma segura ocultando su contenido a posibles fisgones. Una de las ramas de la criptografía que más ha revolucionado el panorama actual de las tecnologías informáticas es el de la firma digital: tecnología que busca asociar al emisor de un mensaje con su contenido de forma que aquel no pueda posteriormente repudiarlo.[28]

En criptografía lo que debe protegerse se denomina *texto en claro***.** El *cifrado* es el proceso de convertir el *texto plano* en un texto ilegible, denominado *texto cifrado* o *criptograma*. Por lo general, la aplicación concreta del *algoritmo de cifrado* (también llamado *cifra*) se basa en la existencia de una *clave*: información secreta que adapta el *algoritmo de cifrado* para cada uso distinto.

Las dos técnicas más sencillas de *cifrado*, en la criptografía clásica, son la ***sustitución*** (que supone el cambio de significado de los elementos básicos del mensaje -las letras, los dígitos o los símbolos-) y la ***trasposición*** (que supone una reordenación de los mismos); la gran mayoría de las *cifras* clásicas son combinaciones de estas dos operaciones básicas.

El *descifrado* es el proceso inverso que recupera el *texto plano* a partir del *criptograma* y la *clave*. El *protocolo criptográfico* especifica los detalles de cómo se utilizan los *algoritmos* y las *claves* (y otras operaciones primitivas) para conseguir el efecto deseado. El conjunto de *protocolos*, *algoritmos de cifrado*, procesos de gestión de claves y actuaciones de los usuarios, en conjunto es lo que constituyen un *criptosistema*, que es con lo que el usuario final trabaja e interactúa.

Existen dos grandes grupos de *cifras*: los algoritmos que utilizan una única *clave* tanto en el proceso de *cifrado* como en el de *descifrado*, y los que utilizan una

[28] BUSTOS, Pérez Jose Ángel. Criptografía. [en línea]. [Fecha de consulta: 28 de septiembre de 2007]. Disponible en <http://es.tldp.org/Presentaciones/200203jornadassalamanca/jadebustos/conferencia-criptografia.pdf>

clave para *cifrar* mensajes y una *clave* distinta para *descifrarlos*. Los primeros se denominan *cifras simétricas* o de *clave simétrica* y son la base de los algoritmos de cifrado clásico. Los segundos se denominan *cifras asimétricas*, de *clave asimétrica* o de *clave pública* y *clave privada* y forman el núcleo de las técnicas de cifrado modernas.

1.5.6 Firmas digitales[29]. La firma digital es, en la transmisión de mensajes telemáticos y en la gestión de documentos electrónicos, un método criptográfico que asegura la *identidad* del remitente. En función del tipo de firma, puede, además, asegurar la *integridad* del documento o mensaje.

La Ley de Firma digital, que puede ser diferente en cada país, define tres tipos de firma:

- Simple. Incluye un método de identificar al firmante.
- Avanzada. Además de identificar al firmante permite garantizar la integridad del documento. Se emplean técnicas de PKI.
- Reconocida. Es la firma avanzada ejecutada con un DSCF (dispositivo seguro de creación de firma) y amparada por un certificado reconocido (certificado que se otorga tras la verificación presencial de la identidad del firmante).

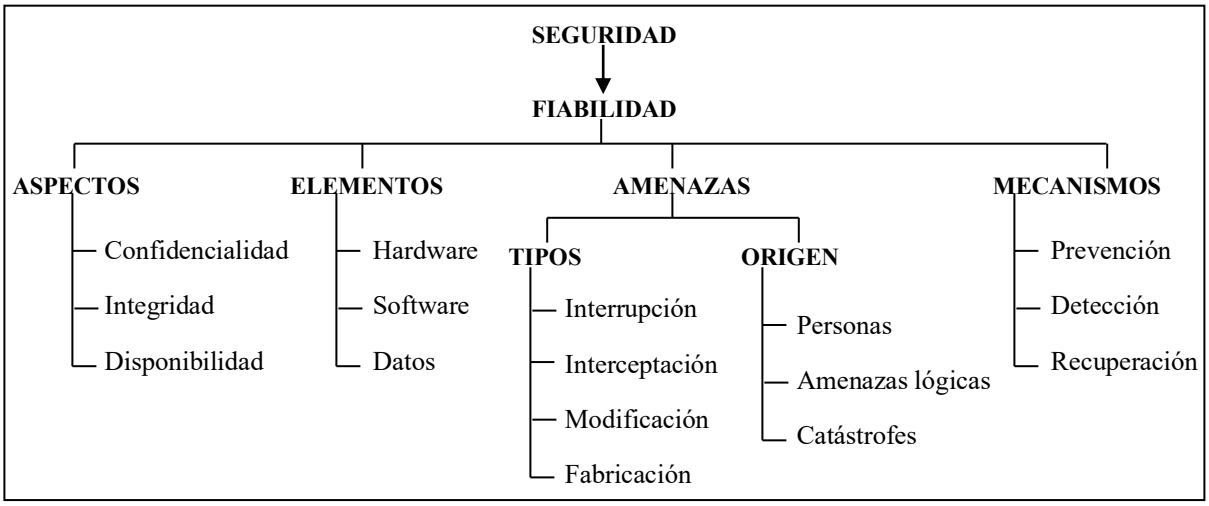
La firma digital de un documento es el resultado de aplicar cierto algoritmo matemático, denominado función hash, a su contenido, y seguidamente aplicar el algoritmo de firma (en el que se emplea una clave privada) al resultado de la operación anterior, generando la firma electrónica o digital.

[29] WIKIPEDIA, La enciclopedia libre. Firma digital [en línea]. [Fecha de consulta: 21 de agosto de 2007].Disponible en <http://es.wikipedia.org/w/index.php?title=Firma_digital&oldid=12370246>

La función hash es un algoritmo matemático que permite calcular un valor resumen de los datos a ser firmados digitalmente, funciona en una sola dirección, es decir, no es posible a partir del valor resumen calcular los datos originales. Cuando la entrada es un documento, el resultado de la función es un número que identifica casi inequívocamente al texto. Si se adjunta este número al texto, el destinatario puede aplicar de nuevo la función y comprobar su resultado con el que ha recibido. No obstante esto presenta algunas dificultades para el usuario, para ello se usan software que automatizan tanto la función de calcular el valor hash como su verificación posterior.

1.6 VISIÓN GLOBAL DE LA SEGURIDAD INFORMÁTICA

Figura 7. Visión Global de La Seguridad Informática.



Fuente: MARTINEZ, Luis David, Seguridad de los sistemas operativos. [en línea]. [Fecha de consulta: 20 de marzo de 2007]. Disponible en: http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/MonogSO/SEGUNIX012.htm

2. DESARROLLO DEL PRODUCTO FINAL

2.1 HERRAMIENTAS DE SOFTWARE LIBRE EMPLEADAS PARA LAS PRUEBAS DE SEGURIDAD

La Seguridad siempre ha sido de lo más importante para los administradores de sistemas. Sin embargo, con la "explosión" del Internet, el riesgo de intrusión se ha vuelto aún más alto. Según la estadística, si el número de usuarios conectados crece, el número de piratas sigue el mismo incremento. Por consecuencia, el desarrollo de software de seguridad ha crecido exponencialmente.[30]

A continuación se dará una explicación concreta y útil sobre algunas herramientas empleadas para el desarrollo del presente proyecto de grado.

2.1.1 Nessus. Es una herramienta que ha estado disponible para su uso durante mucho tiempo, desde 1998. De hecho, esta disponible para Linux, FreeBSD, Solaris, MAX OS X, y Windows (2000, XP, y 2003). La herramienta Nessus abarca dos componentes fundamentales: El servidor y el cliente.

El servidor se encarga de realizar el escaneo real, mientras que el cliente es usado para configurar y hacer que funcionen los escaneos, para visualizar los resultados de loes escaneos y exploraciones realizadas.

Nessus es una herramienta que esta dotada de características variadas, complejas y aplicables, que le permiten realizar más de 10.000 tipos de escaneos

[30] TARBOURIECH, Georges. Herramientas de Seguridad. [en línea]. [Fecha de consulta: 1 de septiembre de 2007].Disponible en <http://es.tldp.org/LinuxFocus/pub/mirror/LinuxFocus/Castellano/January2001/article180.shtml>

y chequeos sobre las vulnerabilidades de las redes, gracias a la capacidad que tiene para descargar plugins y actualizaciones a su base de datos de vulnerabilidades conocidas.

En cuanto al licenciamiento de la herramienta, se puede decir que es relativamente generoso, pero existen algunos casos donde se debe pagar para obtener el licenciamiento de la herramienta. De hecho, usted puede escanear sus sistemas personales, pero cuando va a escanear la tercera parte de la red, una licencia adicional es requerida.

Nessus es usado para el escaneo de redes y agujeros de seguridad en distintos sistemas operativos. Además de escanear puertos, escanea vulnerabilidades utilizando plugins, en constante actualización, escritos en NASL, que es un lenguaje scripting optimizado para interacciones en redes. Está compuesto por dos partes: cliente y servidor, que normalmente se instalan en la misma máquina pero que pueden ser muy útiles por separado para gestión remota de seguridad de redes.

Tiene varias funciones de escaneo en las que se encuentra una muy potente denomina no segura, en la que utiliza diversos exploits esta función pueden causar caídas en sistemas o corromperlos, es recomendable usarla con mucho cuidado. Sus resultados pueden exportarse en mucho formatos, además se incluyen en una base de datos en la que se pueden comparar entre si. Nessus es compatible con los siguientes sistema operativos Linux, FreeBSD, Solaris, Mac OS X y Windows 2000, XP y 2003 (32 bits).

Nessus (Para Unix) consiste en *nessusd*, el daemon Nessus, que realiza el escaneo en el sistema objetivo, y *nessus*, el cliente (basado en consola o gráfico) que muestra el avance y reporte de los escaneos. Desde consola *nessus* puede ser programado para hacer escaneos programados con *cron*.

En operación normal, Nessus comienza escaneando los puertos con Nmap o con su propio escaneador de puertos para buscar puertos abiertos y después intentar varios exploits para atacarlo. Las pruebas de vulnerabilidad, disponibles como una larga lista de plugins, son escritos en NASL, un lenguaje scripting optimizado para interacciones personalizadas en redes.

Para Windows, Nessus 3 se instala como ejecutable, y tiene sus propios contenidos de escaneo, reportes y administración.

Opcionalmente, los resultados del escaneo pueden ser exportados en reportes en varios formatos, como texto plano, XML, HTML, y LaTex. Los resultados también pueden ser guardados en una base de conocimiento para referencia en futuros escaneos de vulnerabilidades.

Algunas de las pruebas de vulnerabilidades de Nessus pueden causar que los servicios o sistemas operativos se corrompan y caigan. El usuario puede evitar esto desactivando "unsafe test" (pruebas no seguras) antes de escanear.

En resumen, Nessus tiene como meta principal, detectar las vulnerabilidades o debilidades potenciales y/o confirmadas en las máquinas que son escaneadas. Por ejemplo:

a. Vulnerabilidades que permiten que un cracker remoto tome control de la máquina o acceda a los datos sensibles almacenados en la misma.

b. Configuraciones defectuosas hechas en la red.

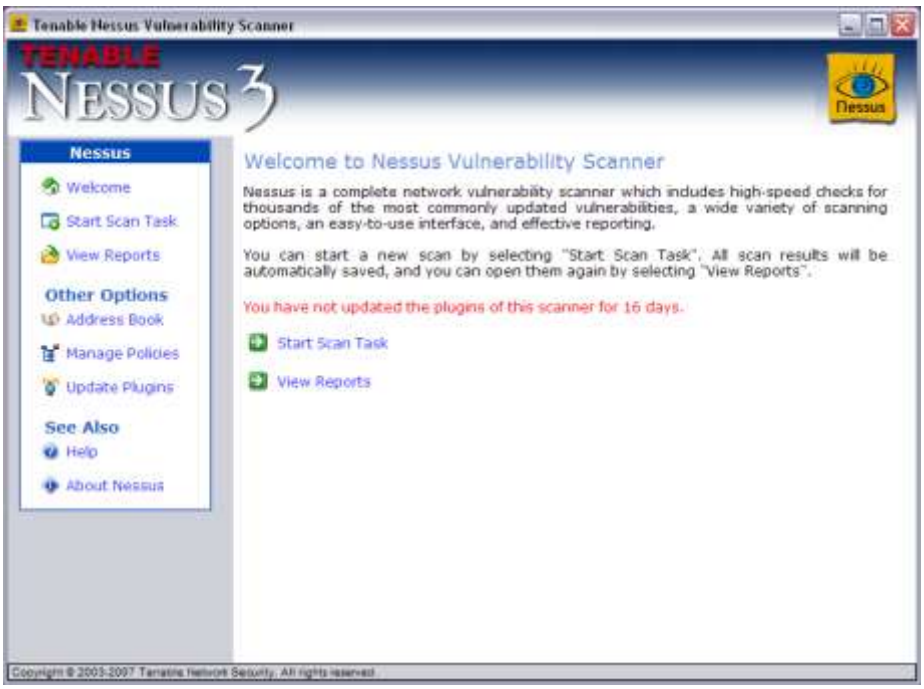
c. Parches de seguridad no implementados.

d. Contraseñas defectuosas (Contraseñas con poco nivel de seguridad e incluso sistemas con contraseñas en blanco).

e. Denegación de servicio en contra la pila TCP/IP.

La Figura No. 8 muestra la interfaz gráfica de usuario de la herramienta Nessus 3 empleada para el escaneo de vulnerabilidades y debilidades en las redes de computadoras.

Figura 8. Interfaz gráfica de usuario de Nessus 3.



Fuente: Autores del proyecto

2.1.2 Nmap. Nmap es una herramienta multiplataforma de código abierto diseñada y usada para explorar grandes redes y obtener información acerca de los servicios, sistemas operativos y vulnerabilidades derivadas de la unión de

éstos, teniendo como función principal el de escanear los puertos y conexiones disponibles que están activas en un determinado equipo.

Nmap se dio a conocer en septiembre de 1997, en un artículo de la revista Phrack Magazine donde incluía el código fuente. Otros desarrollos incluyeron mejores algoritmos para determinar qué servicios estaban funcionando, reescritura de código de C a C++, se agregaron tipos de escaneos adicionales y nuevos protocolos como IPv6. Con el tiempo Nmap ha tenido perfeccionamientos y ha lanzado la versión 3.5 que apareció en febrero de 2004, y la versión 4.0 en enero de 2006, con cientos de mejoras.[31]

Esta herramienta puede funcionar en ambas distribuciones de sistemas operativos como las diversas variables de Unix (Linux, Solaris, Mac OS X, y BSD), y Microsoft Windows, con la diferencia que para su funcionamiento en Windows se necesita el controlador de captura de paquetes, WinPcap. Nmap se encuentra disponible en versión gráfica y de consola, esta utilidad funciona de la misma manera para ambos sistemas operativos, sin embargo hay una diferencia que puede ser significativa, que es la velocidad al escanear la red. Nmap funciona más rápido en Linux que en Windows. En una red pequeña se podría pensar que es de poca consideración, pero al escanear grandes redes la diferencia en tiempo puede llegar a ser muy significativo.

Esta herramienta de escaneo es muy usada por todo aquél que se interesa por las tareas de seguridad y hacking en general, desde Administradores de Sistemas a interesados con fines menos respetables. Las técnicas de escaneo que usa Nmap han sido ya implementadas en sistemas de detección de intrusos y firewalls, ya que los desarrolladores de sistemas de seguridad también usan Nmap en su trabajo y toman medidas. No obstante, pese a estar ampliamente documentado su

[31] WIKIPEDIA, La enciclopedia libre. Nmap [en línea]. [Fecha de consulta: 9 de septiembre de 2007]. Disponible en <http://es.wikipedia.org/w/index.php?title=Nmap&oldid=12399383>

funcionamiento, hay formas de escaneo que lo hacen difícil de detectar cuando se trata de obtener información.

Nmap utiliza paquetes IP "crudos" («raw», N. del T.) en formas originales para determinar qué equipos se encuentran disponibles en una red, qué servicios (nombre y versión de la aplicación) ofrecen, qué sistemas operativos (y sus versiones) ejecutan, qué tipo de filtros de paquetes o cortafuegos se están utilizando así como docenas de otras características. Aunque generalmente se utiliza Nmap en auditorías de seguridad, muchos administradores de redes y sistemas lo encuentran útil para realizar tareas rutinarias, como puede ser el inventariado de la red, la planificación de actualización de servicios y la monitorización del tiempo que los equipos o servicios se mantiene activos.[32]

Nmap cuenta con diferentes tipos de servicios a la hora de realizar escaneos de la red, entre ellos nombramos los más utilizados:[33]

a. *Identificar host activos.* Se realiza este tipo de escaneo cuando se desea saber que host activos se encuentran en la red, para ello se cuenta con el siguiente comando: *#nmap -sP 192.168.0.1-255*

b. Latencia en la red. Se utiliza cuando contamos con una red muy lenta o que maneja mucho tráfico o por el contrario seamos nosotros los que lo generamos, por lo tanto el tiempo de latencia aumenta. Para disminuir el tiempo de búsqueda que utiliza Nmap se utiliza la opción -T indica la política de tiempo a usar, existen 6 niveles con números entre 0-5, cuanto más alto más rápido, por defecto Nmap utiliza -T3. Ejemplo: *#nmap -T5 192.168.1.0/24*

[32] INSECURE.Org. Guía de referencia de Nmap (Página de manual). [en línea]. [Fecha de consulta: 9 de septiembre de 2007]. Disponible en >http://insecure.org/nmap/man/es/index.html>

[33] THE WIL FAMILY. Nmap a fondo: Escaneo de redes y hosts. Junio 27, 2007. [en línea]. [Fecha de consulta: 9 de septiembre de 2007]. Disponible en <http://www.thewilfamily.com/hacking/nmap-a-fondo-escaneo-de-redes-y-hosts>

c. *Descubriendo servicios en un host.* Se realiza al escanear los puertos del host objetivo, Nmap por defecto escanea los puertos menores de 1024 más los que aparecen en el archivo nmap-services y que son mayores de 1024.

d. *Sondeos sigilosos.* Consiste en enviar un paquete *TCP SYN* al puerto a comprobar, y si hay algún servicio activo, el sistema escaneado continuará con la secuencia de conexión enviando un paquete *TCP/SYN*.

e. Fingerprinting. Este escaneo se utiliza para averiguar el sistema operativo del host objetivo usando las pequeñas diferencias en la implementación de los protocolos.

Como se logra observar, Nmap cuenta con gran cantidad de opciones al realizar escaneos, aunque en la pagina principal de Nmap encontramos todos los diferentes comandos para realizar los escaneos en la tabla No. 2 se mencionan los mas útiles y comunes.

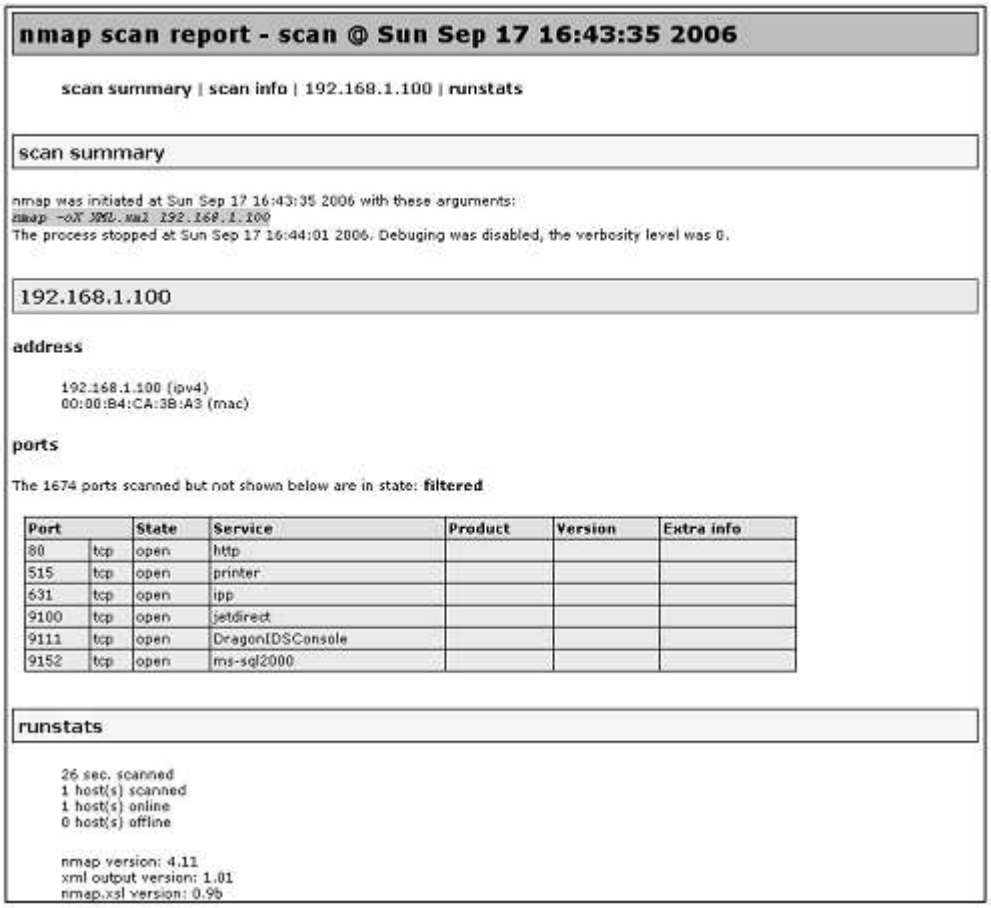
Tabla 2. Opciones de Nmap

Nmap Options		
Option	**Example**	**Notes**
--exclude --excludefile	nmap 192.168.1.1-254 --exclude 192.168.1.106 nmap 192.168.1.1-254 --excludefile file1.txt	These are especially important when scanning large blocks of IP addresses so you can avoid certain critical servers.
-sP	nmap 192.168.1.1-254 -sP	Performs an ICMP ping scan only.
-sV	nmap 192.168.1.1-254 -sV	Attempt to determine service/version on open ports.
-sT	nmap 192.168.1.1-254 -sT	Performs TCP scan using 3-way handshake for each port
-p	nmap 192.168.1.106 -p135,136,137 nmap 192.168.1.106 -p U:514,T:514	Scan only the ports you specify, using TCP or UDP. U:<UDP ports>, T:<TCP ports>
-P0	nmap 192.168.1.1-254 -P0	Treat all hosts as online. Without this, Nmap will not scan the host if it fails to respond to a ping.
-O	nmap 192.168.1.1-254 -O	Perform OS detection.
-A	nmap 192.168.1.1-254 -A	Determine OS and Version info, same as -O and -sV
-oN <file>	nmap 192.168.1.1-254 -oN normal.txt	Sends the same output you would see on screen to a file.
-oX <file>	nmap 192.168.1.1-254 -oX XML.xml	Sends the output in XML format for web viewing.
-oG <file>	nmap 192.168.1.1-254 -oG grepable.txt	Sends the output in a more easily grep'ed format. Grep is the *nix command line filtering utility, similar in functionality to the Windows find utility.
-v or -vv	nmap 192.168.1.106 -v nmap 192.168.1.106 -vv	More verbose output providing more detail about what actions Nmap is performing.

Fuente: Rave Alder, Josh Burke, Chad Keefer, Angela Orebaugh, Larry Pesce y Erick S. Seagren. How to cheat at configuring open source security tools [E-Book]. Singress. Nmap.

Nmap permite guardar los resultados de un escaneo en un archivo XML, que llega a ser muy útil a la hora de presentar informes de los resultados del escaneo realizado, como se muestra en la imagen a continuación (Ver Figura No. 9).

Figura 9. Salida de escaneo en formato XML



nmap scan report - scan @ Sun Sep 17 16:43:35 2006

scan summary | scan info | 192.168.1.100 | runstats

scan summary

nmap was initiated at Sun Sep 17 16:43:35 2006 with these arguments:
nmap -oX XML.xml 192.168.1.100
The process stopped at Sun Sep 17 16:44:01 2006. Debuging was disabled, the verbosity level was 0.

192.168.1.100

address

192.168.1.100 (ipv4)
00:00:B4:CA:3B:A3 (mac)

ports

The 1674 ports scanned but not shown below are in state: filtered

Port		State	Service	Product	Version	Extra info
80	tcp	open	http			
515	tcp	open	printer			
631	tcp	open	ipp			
9100	tcp	open	jetdirect			
9111	tcp	open	DragonIDSConsole			
9152	tcp	open	ms-sql2000			

runstats

26 sec. scanned
1 host(s) scanned
1 host(s) online
0 host(s) offline

nmap version: 4.11
xml output version: 1.01
nmap.xsl version: 0.9b

Fuente. Rave Alder, Josh Burke, Chad Keefer, Angela Orebaugh, Larry Pesce y Erick S. Seagren. How to cheat at configuring open source security tools [E-Book]. Singress. Nmap.

Nmap es una muy buena herramienta para escaneos de seguridad en la red y puede ser descargado de su página oficial http://www.insecure.org/nmap/. Para

mayor información a cerca de la herramienta puedes observar el manual en español que se encuentra en http://insecure.org/nmap/man/es/.

2.1.3 VNC - Virtual Network Computing. VNC es un software propiedad de la británica RealVNC. Se compone de un servidor y un cliente (visor) que permite interactuar con el escritorio de entornos Windows, Linux, Solaris y HP-UX desde cualquier plataforma a su vez. Es un software tremendamente extendido (más de 100 millones de descargas desde 1998) entre los administradores de red, debido a su sencillez, potencia y sobre todo, el hecho de estar licenciado bajo GPL.

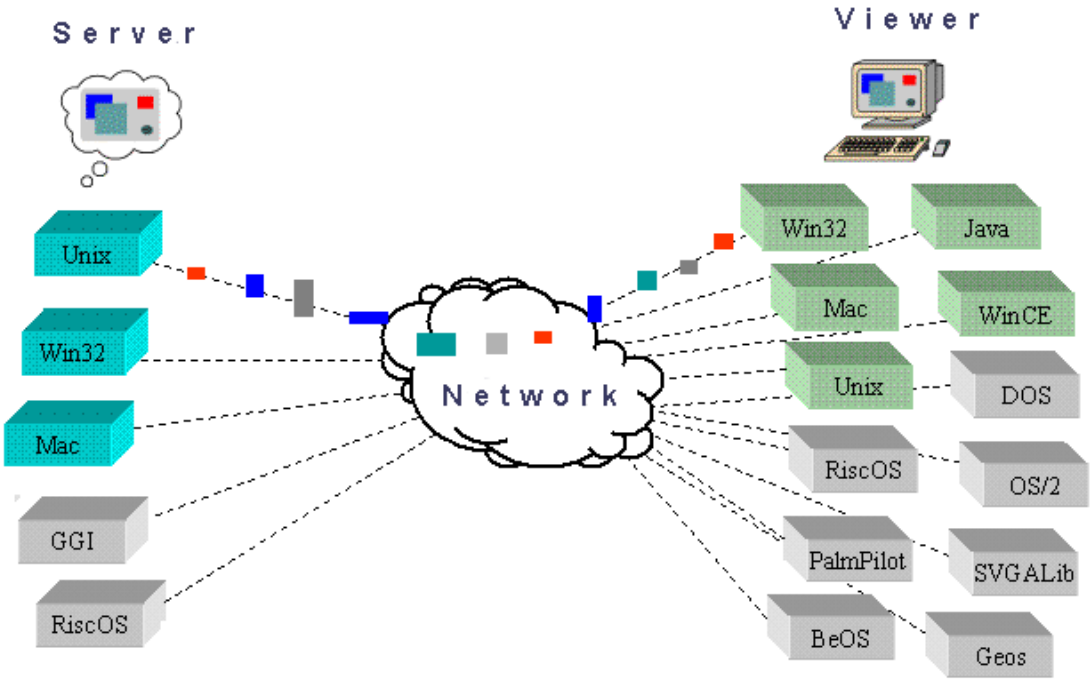
Es un programa de software libre basado en una estructura cliente-servidor el cual permite tomar el control del computador servidor remotamente a través de un computador cliente. También llamado software de escritorio remoto. VNC permite que el sistema operativo en cada computadora sea distinto. Es posible compartir la pantalla de una máquina con Windows en una máquina con GNU/Linux y viceversa.

Este software de control remoto, permite ver e interactuar completamente con un computador de escritorio ("Servidor VNC") usando un simple programa ("Visor VNC") en otro computador de escritorio conectado a Internet. Los dos computadores incluso, no necesariamente tienen que ser del mismo tipo. Por ejemplo, puede usar VNC para ver un computador con sistema operativo Windows Vista desde un computador con sistema operativo Linux. (Ver Figura No. 10). Además, existe un visor de Java, que permite que un computador sea controlado remotamente desde un browser, sin la necesidad de instalar previamente software.

VNC es un software que actualmente esta siendo utilizado por millones de personas en diversos campos, tales como la industria y la academia. Además,

existen variadas versiones para elegir, incluyendo la versión libre y versiones comerciales de este software.

Figura 10. Funcionamiento de VNC.



Fuente: RealVNC. [en línea]. [Fecha de consulta: 25 de Marzo de 2007]. Disponible en: <http://www.realvnc.com/vnc/index.html>

VNC tiene una amplia gama de usos, incluyendo administración de sistemas, apoyo a tecnologías de la información y helpdesk. Igualmente, el sistema permite varias conexiones para el mismo computador, permitiendo tener una herramienta invaluable para la colaboración o el trabajo compartido en una oficina o en un salón de clases.

Para un usuario individual, un escenario común de uso seria permitirle la ayuda remota a otro usuario ubicado geográficamente en otra zona. Por ejemplo, un usuario ubicado en Bucaramanga, podría usar VNC para tomar el control del otro computador ubicado en Bogotá, y mostrarle como instalar un nuevo software y de que manera usar este nuevo software haciéndolo de manera remota.

Un uso común de VNC en los negocios y empresas es la administración remota, que es usada para permitir a los administradores de la red tomar el control de los computadores de los empleados para diagnosticar problemas y repararlos, o para tener acceso y administrar servidores sin la necesidad de estar físicamente presente frente a la consola.

De otro lado, VNC es usado en contextos institucionales y educativos, para permitir a un grupo de estudiantes ver en las pantallas de su computadores algo específico y que pueda se manipulado por el instructor o docente para mantener el control de la clase. Del mismo modo, es usado para proveer ayuda a los estudiantes mediante el acceso y control de su computador.

En realidad, los ejemplos nombrados anteriormente, son unos de los pocos usos que puede brindar VNC a millones de usuarios.

- **Vulnerabilidad en RealVNC[34].** Steve Wiseman descubrió, casi por casualidad, una importante vulnerabilidad en VNC; un software de administración remota muy usado en distintos sistemas operativos que permite interactuar con el escritorio de cualquier sistema. El fallo puede hacer que se eluda de forma sencilla la autenticación y acceder al equipo con el servidor instalado sin necesidad de conocer la contraseña.

[34] HISPASEC Sistemas. Seguridad y tecnologías de la información. Grave Vulnerabilidad en RealVNC. Publicado el 15/05/2006. [en línea]. [Fecha de consulta: 10 de septiembre de 2007]. Disponible en <http://www.hispasec.com/unaaldia/2760>

VNC suele abrir un puerto (5900/TCP/UDP - VNC Server) al exterior para que remotamente el administrador pueda interactuar con cualquier sistema como si estuviese sentado frente el escritorio de un computador que puede encontrarse físicamente a miles de kilómetros de distancia. El software ha sido incluido en distintas distribuciones de Linux y forma parte de otros paquetes de software. Para los sistemas que ofrezcan abiertamente el servicio hacia Internet, el hecho de que esté protegido por contraseña pierde el sentido ante este fallo y queda virtualmente a disposición de quien conozca los detalles de la vulnerabilidad.

Debido a la importancia del descubrimiento, Wiseman casi no podía creerlo. Mientras programaba un cliente propio para conectarse a servidores VNC, se dio cuenta de que podía acceder al servidor sin conocer la contraseña. Trabajaba con VNC Free Edition 4.1.1 bajo Windows y, después de muchas pruebas para asegurase de que lo que tenía ante sus ojos suponía un grave problema, no pudo más que concluir que realmente estaba ante una gravísima vulnerabilidad.

Tras unos momentos de pánico, en los que Wiseman descargó los "hermanos" de VNC TightVNC y UltraVNC y comprobó que no eran vulnerables, se puso en contacto con RealVNC y al poco tiempo hicieron disponible la versión no vulnerable 4.1.2.

El fallo se debe a un error de diseño en el proceso de autenticación, mientras el cliente y el servidor llegan a un acuerdo sobre el tipo de autenticación. Uno de estos tipos de autenticación disponibles desde el servidor es precisamente la no autenticación, donde no se pedirá contraseña al cliente. Una implementación incorrecta permite que sea el cliente el que elija el tipo, independientemente del que tenga configurado el propio servidor, de entre un array que éste hace disponible durante la negociación. De esta forma, sólo es

necesario cambiar un poco la información que el cliente envía, y será el propio cliente el que tenga la posibilidad de elegir "no autenticación" para acceder al servidor, aunque se encuentre en realidad protegido por contraseña.

Aunque no se han dado detalles técnicos sobre el problema, según se publica en listas de seguridad, es trivial reproducir el fallo, y cuestión de tiempo que aparezca un cómodo exploit capaz de acceder a cualquier servidor que ejecute este popular programa.

2.1.4 RPC - Remote Procedure Call. Es un protocolo que permite a un programa de computador ejecutar código en otra máquina remota sin tener que preocuparse por las comunicaciones entre ambos. El protocolo es un gran avance sobre los sockets usados hasta el momento. De esta manera el programador no tenía que estar pendiente de las comunicaciones, estando éstas encapsuladas dentro de las RPC.

Las RPC son muy utilizadas dentro del paradigma cliente-servidor. Siendo el cliente el que inicia el proceso solicitando al servidor que ejecute cierto procedimiento o función y enviando éste de vuelta el resultado de dicha operación al cliente.

- **Vulnerabilidad RPC/DNS[35].** El problema de dar paso a esta vulnerabilidad se debe a un desbordamiento de memoria intermedia en la implementación de la interfaz RPC del servidor DNS (Domain Name System) de Windows a la hora de procesar peticiones mal formadas. Esto puede ser aprovechado por atacantes para ejecutar código arbitrario con privilegios de SYSTEM (control

[35] HISPASEC SISTEMAS. Detalles y evolución de la vulnerabilidad RPC/DNS de Microsoft Windows [en línea]. 17 de abril de 2007 [Fecha de consulta: 11 de septiembre de 2007]. Disponible en: <http://www.hispasec.com/unaaldia/3097>

total sobre el sistema) si se envía una petición especialmente manipulada al sistema vulnerable.

Esto afectaría a un sistema sólo si mantiene un DNS (típicamente en servidores de Microsoft), y un potencial atacante tuviese acceso a unos puertos específicos. El ataque no sería posible exclusivamente a través del puerto 53, abierto habitualmente al exterior para las consultas DNS, sino que debe apoyarse de la capacidad de administración remota de DNS (a través de RPC) para explotar la vulnerabilidad y ejecutar código. Microsoft proporcionó un método para eliminar esta funcionalidad y proteger el sistema a falta de parche oficial.

Aun así, varios factores se han añadido a la ecuación para convertir esta vulnerabilidad en un verdadero peligro. Típicamente un controlador de dominio en red interna es también el servidor autorizado DNS del dominio. En una red interna, no suelen protegerse estos controladores tras un cortafuegos, o las reglas de filtrado pueden estar más relajadas. En ese caso, aunque no expuesto al exterior, el servidor podría quedar fácilmente comprometido desde la misma red interna. Si el controlador de dominio queda comprometido, el atacante habría llegado al corazón de una red interna controlada por el directorio activo.

2.1.5 LANGuard Network Security Scanner (NSS)[36]. Es una solución desarrollada por GFI que permite escanear, detectar, evaluar y remediar cualquier vulnerabilidad de seguridad de las redes.

[36] GFiLANguard. Network Security Scanner. Escáner de vulnerabilidad, gestión de parches y auditoria de red [en línea]. [Fecha de consulta: 12 de septiembre de 2007]. Disponible en: <http://www.gfihispana.com/es/lannetscan/lanscanbrochure_es.pdf>

Esta solución comprueba la red, a través de la realización de todos los posibles métodos de ataque que un hacker podría utilizar para atacarla. A través del análisis del sistema operativo y las aplicaciones que se ejecutan en sus máquinas de red, GFI LANguard Network Security Scanner determina todas las posibles brechas de seguridad en la red. En otras palabras, hace de abogado del diablo, y le alerta de las debilidades y vulnerabilidades antes de que un hacker pueda encontrarlas, permitiéndole tratarlas antes de que sean aprovechadas.

LANguard facilita la tarea de los administradores de la red. Esta herramienta se encarga tratar los problemas referentes a seguridad, la administración de parches y auditoria de red; todo en uno, a través de una única solución y un único paquete software. Dicha solución integrada GFI LANguard N.S.S. le ayuda a abordar estos asuntos más rápida y eficazmente.

GFI LANguard N.S.S. hace uso de avanzadas bases de datos de vulnerabilidades basadas en OVAL y en SANS TOP 20, proporcionando más de 15.000 valoraciones de vulnerabilidades cuando su red es escaneada. GFI LANguard N.S.S. le da la información y las herramientas que necesita para realizar escaneos multiplataforma a través de todos los entornos, para analizar el estado de la seguridad de su red y para instalar y administrar eficazmente los parches de todos los equipos a través de diferentes sistemas operativos y en diferentes idiomas. Esto da como resultado un entorno consistentemente configurado que es seguro contra todas las vulnerabilidades.

GFI LANguard N.S.S. es la más completa solución de administración de vulnerabilidades en un paquete convenientemente integrado. GFI LANguard N.S.S. es una solución empresarial esencial y rentable para salvaguardar sistemas y redes de ataques hacker y brechas de seguridad.

A continuación se nombran y se detallan algunas de las características y/o beneficios de LANguard.

- **Solución integrada de administración de vulnerabilidades.** GFI LANguard Network Security Scanner (N.S.S.) es una premiada solución que dirige los tres pilares de la gestión de vulnerabilidades (Ver Figura No. 11): análisis de seguridad, administración de parches y auditoria de red mediante una única e integrada consola. A través del escaneo de toda la red, identifica todos los posibles problemas de seguridad y utilizando sus extensas funcionalidades de generación de informes le proporciona las herramientas que necesita para detectar, valorar, informar y remediar cualquier amenaza.

  - Análisis de vulnerabilidad.
  - Administración de parches.
  - Auditoria de red y de software.

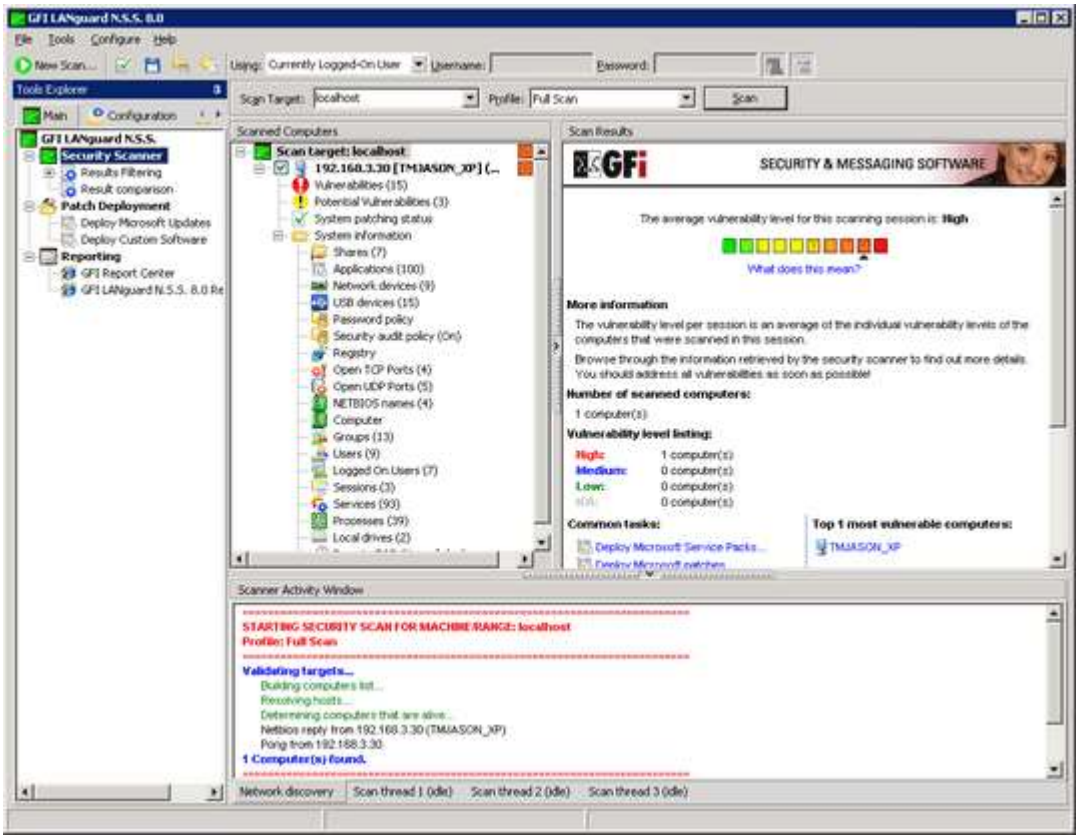
Figura 11. Pilares de la gestión de vulnerabilidades.

Fuente: GFI LANguard Network Security Scanner. [en línea]. [Fecha de consulta: 25 de Marzo de 2007]. Disponible en: <http://www.gfihispana.com/es/lannetscan/lanscanfeatures.htm>

I. ***Análisis de vulnerabilidad.*** Durante las auditorias de seguridad, se realizan más de 15.000 valoraciones de vulnerabilidad y las redes se escanean IP por IP. GFI LANguard N.S.S. le da la capacidad de realizar análisis multiplataforma ((Windows, Mac OS, Linux) a través de todos los entornos y para analizar el estado de la seguridad de la red desde un único origen de datos. Esto asegura que se pueda identificar y remediar cualquier amenaza antes de que los hackers lo logren.

a. *Identifica vulnerabilidades de seguridad y toma medidas correctoras.* Escanea equipos, identifica y clasifica vulnerabilidades de seguridad, recomienda un curso de acción y proporciona herramientas que le permiten resolver estos asuntos. Además, emplea un indicador gráfico, que muestra el nivel de la amenaza a fin de proporcionarle al administrador de la red o equipo, una visión sobre el estado actual de la valoración de la(s) vulnerabilidad(es). Ver Figura No. 12. Pantalla principal de GFI LANguard Network Security Scanner.

Figura 12. Pantalla principal de GFI LANguard Network Security Scanner.



Fuente: GFI LANguard Network Security Scanner. [en línea]. [Fecha de consulta: 25 de Marzo de 2007]. Disponible en: <http://www.gfihispana.com/es/lannetscan/lanscanscreenpop.htm>

b. *Base de datos de vulnerabilidades de gran alcance y potencia industrial.* Tiene una completa base de datos de valoración de vulnerabilidades, la cual se actualiza regularmente con información de diversos estándares (OVAL, SANS Corporation y Bug-Traq, entre otros.).Además, posee un sistema de auto actualización que se encarga de mantener actualizado el software con las últimas actualizaciones liberadas (seguridad de Microsoft, de GFI y almacenes de bases de datos de vulnerabilidades como OVAL).

c. *Asegura que las aplicaciones de seguridad de terceros como anti-virus y anti-spyware ofrecen la protección óptima.* Comprueba que las aplicaciones de seguridad soportadas como anti-virus y anti-spyware están actualizadas con los últimos archivos de definición y que están funcionando correctamente.

d. *Crea fácilmente diversos tipos de análisis y test de vulnerabilidad.* Se pueden configurar fácilmente análisis de diferentes tipos. Además puede analizar diferentes tipos de vulnerabilidades para identificar potenciales problemas de seguridad. Estas incluyen:

- Puertos abiertos: Identificar los puertos que se encuentran abiertos en la red.

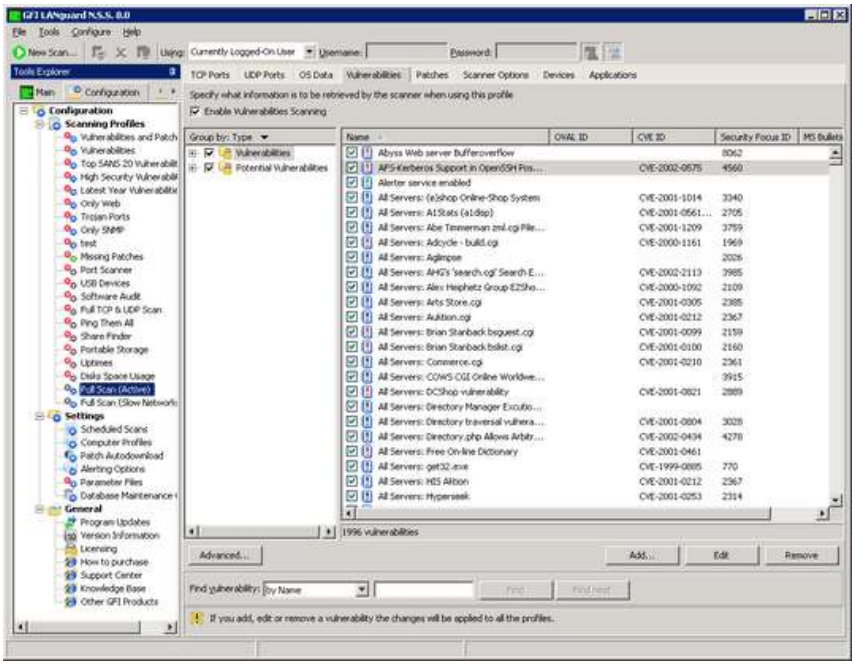
- Usuarios y grupos locales que no se utilizan: Eliminar o deshabilitar cuentas de usuario que ya no se usan.

- Aplicaciones en lista negra: Identificar software no autorizado o peligroso y agregarlo a listas negras de aplicaciones que usted desee asociar con una alerta de vulnerabilidad de alta seguridad.

- Dispositivos USB peligrosos, nodos y enlaces inalámbricos: Busca todos los dispositivos conectados a USB o enlaces inalámbricos y le avisa de cualquier actividad sospechosa.

Los análisis nombrados anteriormente son uno de los pocos tipos de análisis que esta poderosa herramienta permite realizar. Ver Figura No. 13. Configurando las vulnerabilidades a analizar.

Figura 13. Configurando las vulnerabilidades a analizar.



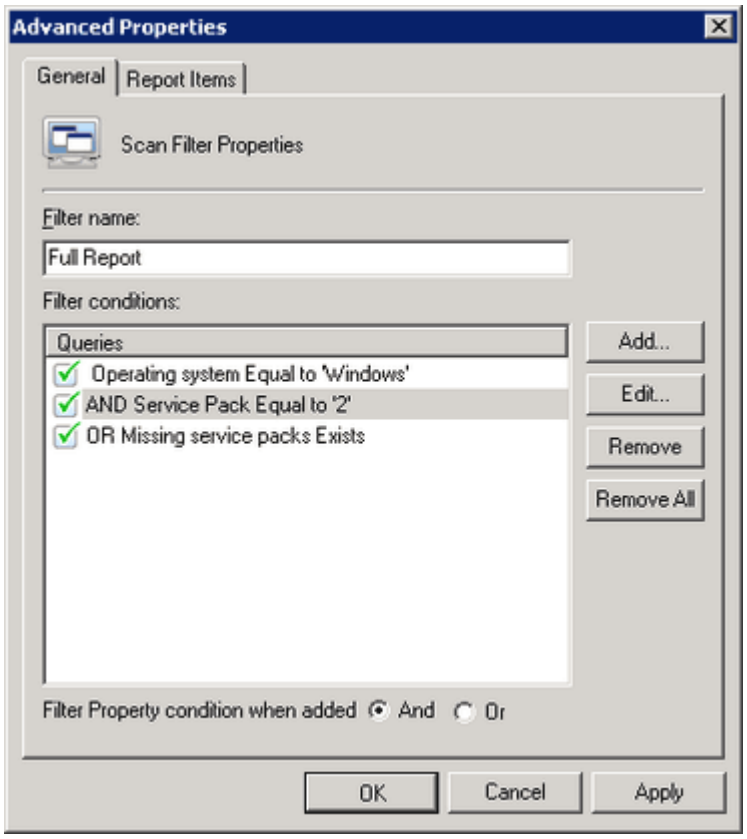
Fuente: GFI LANguard Network Security Scanner. [en línea]. [Fecha de consulta; 25 de Marzo de 2007]. Disponible en: <http://www.gfihispana.com/es/lannetscan/lanscanscreenpop.htm?id=scr_scanpatches>

e. *Crea a medida sus propias evaluaciones de vulnerabilidad.* Crea a medida, evaluaciones de vulnerabilidad mediante un asistente de creación y configuración de una nueva condición de vulnerabilidad.

f. *Analice y filtre fácilmente los resultados del análisis.* Permite analizar y filtrar fácilmente los resultados de los análisis haciendo clic sobre uno de los nodos predefinidos del filtro. Esto le permite identificar, por ejemplo, equipos con vulnerabilidades de alta seguridad o equipos a los que les falte un service pack concreto. También se pueden crear muy fácilmente los filtros personalizados desde un principio o los personalizados.

También puede exportar los resultados a XML. Ver Figura No. 14. Filtre fácilmente los resultados del análisis.

Figura 14. Filtre fácilmente los resultados del análisis.



Fuente: GFI LANguard Network Security Scanner. [en línea]. [Fecha de consulta: 25 de Marzo de 2007]. Disponible en: <http://www.gfihispana.com/es/lannetscan/lanscanscreenpop.htm?id=scr_scanpatches>

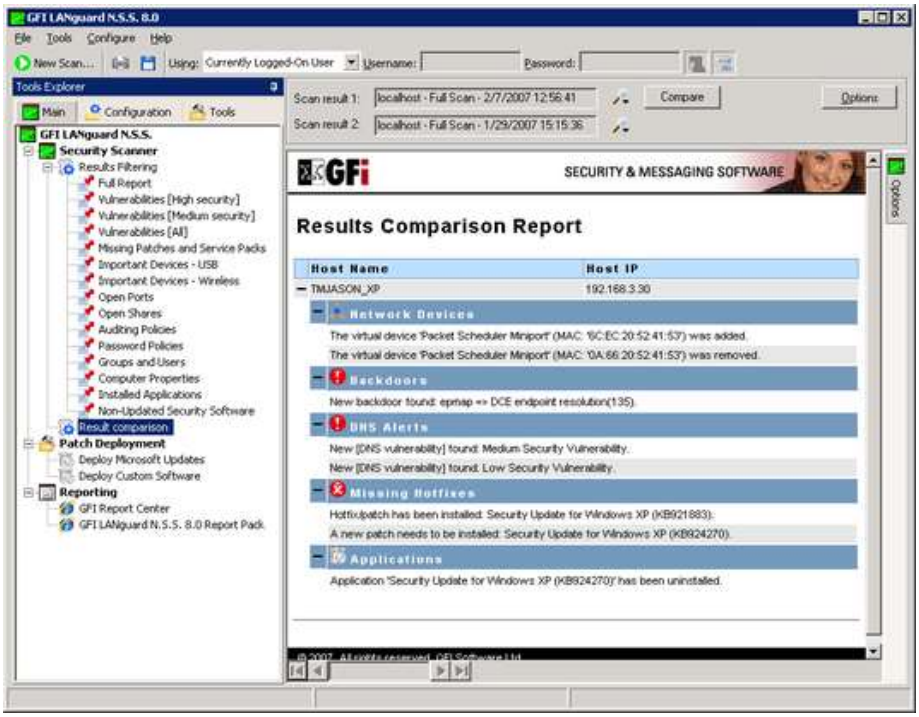
II. ***Administración de Parches.*** Cuando se completa un escaneo, GFI LANguard N.S.S. le da toda la funcionalidad y herramientas que necesita para instalar y administrar eficazmente los parches en todos los equipos a través de diferentes plataformas de sistema operativo y 38 idiomas.

LANguard también permite auto descarga de parches faltantes así como la retirada de parches. Además se puede implantar software de terceros. Esto da como resultado un entorno consistentemente configurado que es seguro contra todas las vulnerabilidades.

III. ***Auditoria de Red y de Software.*** Esta función de LANguard muestra todo lo que necesita saber sobre la red (qué dispositivos USB están conectados, qué software está instalado, cualquier recurso compartido abierto, puertos abiertos y contraseñas débiles en uso). Los informes en profundidad de la solución le proporcionan información importante en tiempo real del estado de su red. Los resultados de los escaneos pueden ser fácilmente analizados utilizando filtros e informes, permitiéndole asegurar proactivamente la red mediante el cierre de puertos, eliminación de usuarios o grupos que ya no se utilizan o deshabilitando los puntos de acceso inalámbricos.

a. *Notificación automática de avisos de nuevas brechas de seguridad.* GFI LANguard N.S.S. puede realizar análisis programados (por ejemplo, diaria o semanalmente) y puede compararlos automáticamente con resultados de análisis anteriores. Cualquier nueva brecha de seguridad o cambio de configuración descubierto en su red le será enviado por correo para su análisis. Esto le permite identificar rápidamente nuevos recursos compartidos, servicios instalados, aplicaciones instaladas, usuarios agregados, nuevos puertos abiertos y más. Ver Figura No. 15. Comparando resultados entre análisis.

Figura 15. Comparando resultados entre análisis.



Fuente: GFI LANguard Network Security Scanner. [en línea]. [Fecha de consulta; 25 de Marzo de 2007]. Disponible en: <http://www.gfihispana.com/es/lannetscan/lanscanscreenpop.htm?id=scr_scanpatches>

b. *Permite comprobar si la auditoria de seguridad está habilitada en toda la red.* GFI LANguard N.S.S. comprueba si cada equipo NT/2000/XP/VISTA tiene habilitada la auditoria de seguridad. Si no, GFI LANguard N.S.S. le avisa y le permite habilitarla remotamente. La auditoria de eventos de seguridad es altamente recomendable porque detecta intrusos en tiempo real.

c. *Analiza y recupera datos de SO de sistemas Linux.* Es posible extraer remotamente datos del SO de sistemas basados en Linux y el resultado se presenta de la misma forma que para equipos basados en Windows.

Esto significa que los equipos Linux y Windows se pueden analizar en una sola sesión de escaneo! GFI LANguard N.S.S. incluye numerosas comprobaciones de seguridad Linux incluyendo detección de rootkit. GFI LANguard N.S.S. puede utilizar archivos de Clave Privada SSH en lugar de las convencionales credenciales de contraseña para autentificarse en equipos Linux.

Para obtener información completa sobre los productos de seguridad desarrollados por GFI, y descargar versiones freeware y demo de sus aplicaciones; consulte el sitio URL: <http://www.gfisoftware.com/lannetscan/>

2.1.6 LCP[37]. Es una herramienta de auditoria y recuperación de contraseñas. Es usada para testear la debilidad de las contraseñas y algunas veces para recuperar las que se han olvidado o perdido en sistemas Microsoft Windows (NT/2000/XP/2003). Esta herramienta utiliza ataques por diccionario, ataques por fuerza bruta, o una combinación de los dos anteriores (ataques híbridos). Ver Figura No. 17, Figura No. 18 y Figura No. 19.

a. *Información sobre el aplicativo, en sus sistemas de importación:*

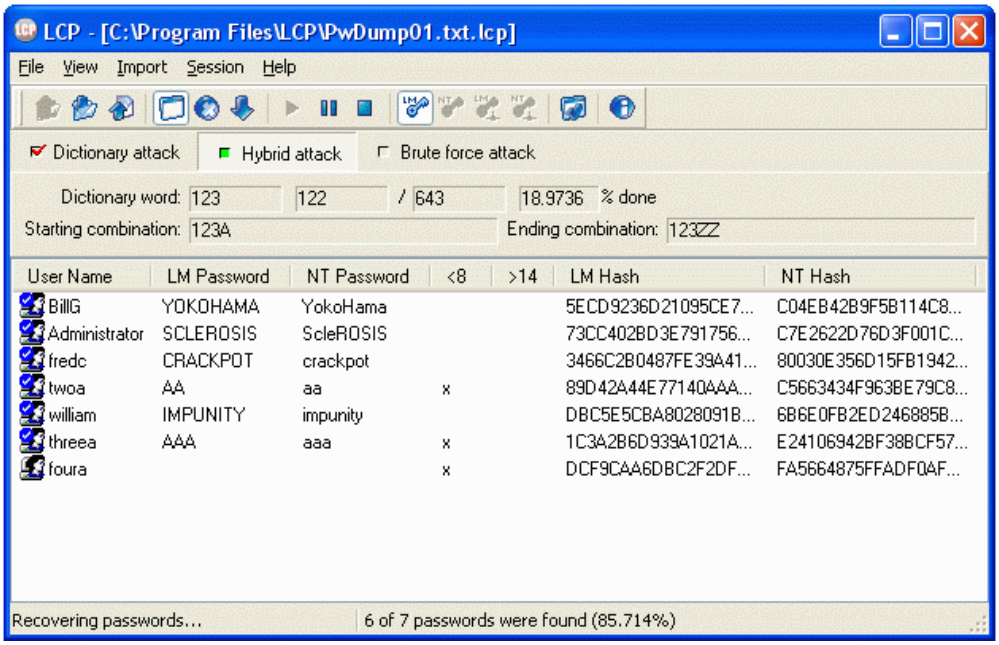
- Permite la importación en Local.
- Importación en remoto.
- Importar Archivo SAM.
- Importar archivos .LC
- Importar archivos .LCS
- Importar archivos desde PwDump.
- Importar desde su sniffer integrado.

[37] LPCSoft [en línea]. [Fecha de consulta: 20 de septiembre de 2007]. Disponible en:<http://www.lcpsoft.com/english/index.htm#lcp>

b. Información sobre el aplicativo en sus sistemas de Recuperación de passwords:

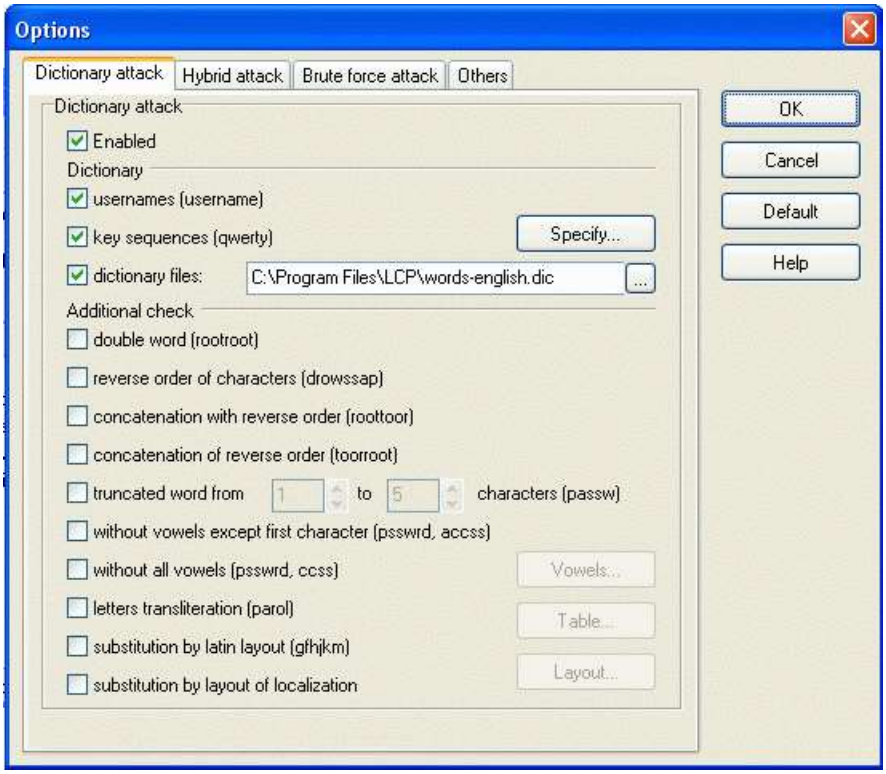
- Ataques por medio de diccionario.
- Ataques Híbridos (diccionario-fuerza bruta).
- Ataques por fuerza bruta.

Figura 16. Pantalla de inicio de LCP.



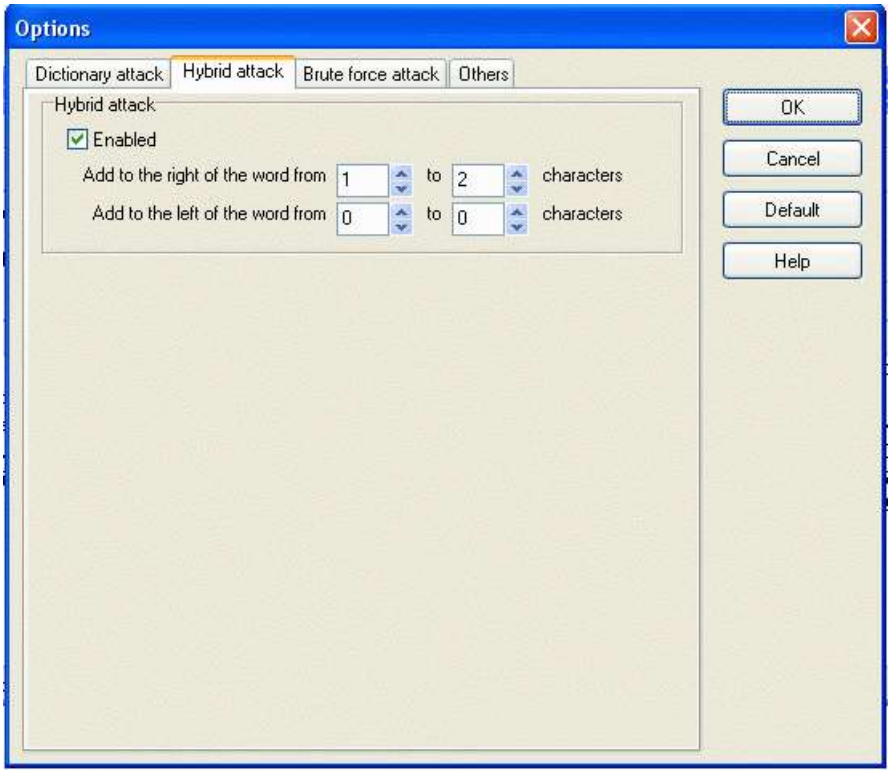
Fuente: DragonJar, Recuperación de contraseñas Windows. [en línea]. [Fecha de consulta: 30 de Marzo de 2007]. Disponible en: http://www.dragonjar.org/lcp-una-buena-opcion-libre-frente-a-l0phtcrack.xhtml

Figura 17. Activación del diccionario de ataques para la recuperación de contraseñas.



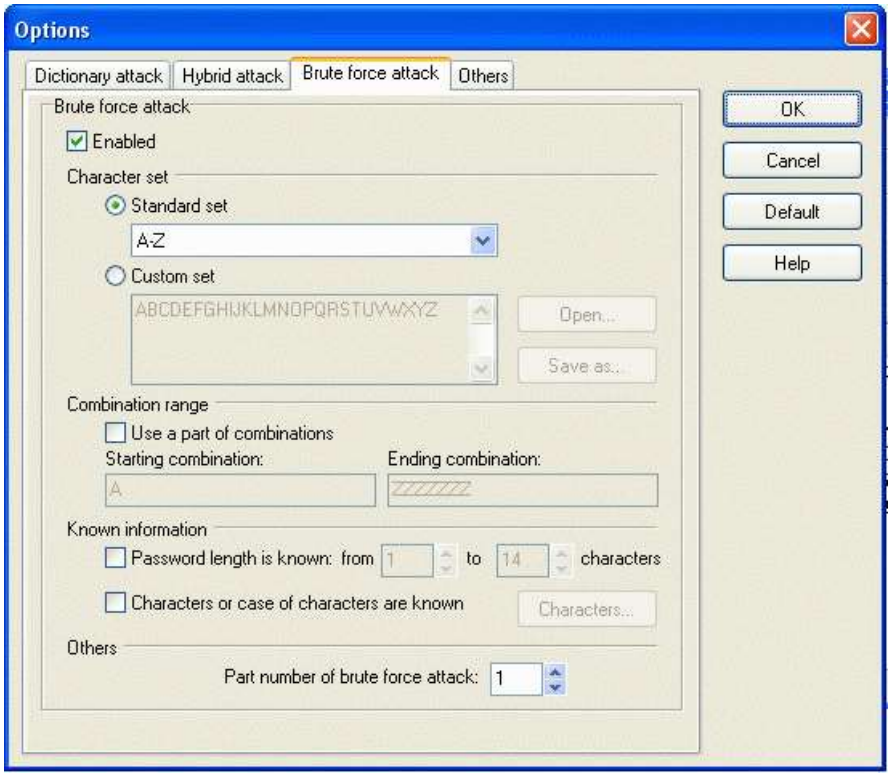
Fuente: DragonJar, Recuperación de contraseñas Windows. [en línea]. [Fecha de consulta: 30 de Marzo de 2007]. Disponible en: http://www.dragonjar.org/lcp-una-buena-opcion-libre-frente-a-l0phtcrack.xhtml

Figura 18. Activación del ataque híbrido para recuperación de contraseñas.



Fuente: DragonJar, Recuperación de contraseñas Windows. [en línea]. [Fecha de consulta; 30 de Marzo de 2007] Disponible en: http://www.dragonjar.org/lcp-una-buena-opcion-libre-frente-a-l0phtcrack.xhtml

Figura 19. Activación de ataque a través de fuerza bruta para recuperación de contraseñas.



Fuente: DragonJar, Recuperación de contraseñas Windows. [en línea]. [Fecha de consulta; 30 de Marzo de 2007]. Disponible en: http://www.dragonjar.org/lcp-una-buena-opcion-libre-frente-a-l0phtcrack.xhtml

2.1.7 Cain & Abel. Es un sniffer, el cual permite recuperar passwords para sistemas operativos de Microsoft. Esta herramienta recupera fácilmente varios tipos de passwords mediante el sniffing de la red, lográndolo por medio de Crackear passwords encriptados usando diccionarios, fuerza bruta y ataques mediante criptoanálisis. También graba conversaciones VoIP, decodifica passwords, recupera claves de red o claves almacenadas en caché. El programa no hace exploit de ninguna vulnerabilidad software, en cambio lo que hace es cubrir algunos aspectos de seguridad presentes en los protocolos estándares, métodos de autentificación y mecanismos de caché. El principal propósito de este

sniffer, es el de recoger passwords de diversos lugares. La herramienta fue pensada para ser utilizada por administradores de redes, profesores, testeadores de intrusiones en el sistema y a cualquier otro profesional de seguridad, más que para ser usada con fines maliciosos.

2.1.8 Ettercap. Es un interceptor/sniffer/registrador para LANs con switch. Soporta disecciones activas y pasivas de varios protocolos (incluso aquellos cifrados, como SSH y HTTPS). También hace posible la inyección de datos en una conexión establecida y filtrado al vuelo aun manteniendo la conexión sincronizada gracias a su poder para establecer un Ataque Man-in-the-middle (Spoofing). Muchos modos de sniffing fueron implementados para dar un conjunto de herramientas poderosas y completas de sniffing.

Además, Ettercap es considerada una de las mejores herramientas para capturar trafico en la red, el cual es muy adaptable, debido a que se pueden crear filtros al gusto del usuario, para capturar el tráfico sobre el cual se esta interesado (Usuario y Contraseña…) en un determinado puerto. Lo grandioso de la herramienta, es la combinación con ataques de envenenamiento de Arp (Arp Spoofing) con lo que se puede lograr pasar por el Gateway s de la red y así capturar el trafico de cualquier computador en la red. Esta herramienta se puede ejecutar en Windows o en Linux.

- **Funciones de Ettercap.**

  a. Inyección de caracteres en una conexión establecida emulando comandos o respuestas mientras la conexión está activa.

  b. Compatibilidad con SSH1: puede interceptar usuarios y contraseñas incluso en conexiones "seguras" con SSH.

c. Compatibilidad con HTTPS: intercepta conexiones mediante http SSL (supuestamente seguras) incluso si se establecen a través de un proxy.

d. Intercepta tráfico remoto mediante un túnel GRE: si la conexión se establece mediante un túnel GRE con un router Cisco, puede interceptarla y crear un ataque "Man in the Middle".

e. "Man in the Middle" contra túneles PPTP (*Point-to-Point Tunneling Protocol*).

Ettercap es un sniffer capaz de ejecutarse en cualquiera de las siguientes plataformas:

- Linux 2.0.x
- Linux 2.2.x
- Linux 2.4.x
- Linux 2.6.x
- FreeBSD 4.x 5.x
- OpenBSD 2.[789] 3.x
- NetBSD 1.5
- Mac OS X (darwin 1.3 1.4 5.1 6.x 7.x)
- Windows 9x
- Windows NT
- Windows 2000
- Windows XP
- Solaris 2.x

2.2 HERRAMIENTAS DE SOFTWARE LIBRE RECOMENDADAS PARA MANTENER LA SEGURIDAD DE LA RED

2.2.1 Sistemas de detección de intrusos.

- **Tcpdump.** Es una herramienta en línea de comandos cuya utilidad principal es analizar el tráfico que circula por la red.

  Tcpdump permite al usuario capturar y mostrar a tiempo real los paquetes transmitidos y recibidos en la red a la cual el computador está atado. Tcpdump funciona en la mayoría de los sistemas operativos UNIX: Linux, Solaris, BSD, Mac OS X, HP-UX y AIX entre otros. En esos sistemas, hace uso de la librería libpcap para capturar los paquetes que circulan por la red.

  Existe una adaptación de Tcpdump para los sistemas Windows que se llama WinDump y que hace uso de la librería Winpcap.

  En UNIX y otros sistemas operativos, es necesario tener los privilegios del root para utilizar Tcpdump.

  El usuario puede aplicar varios filtros para que sea más depurada la salida. Un filtro es una expresión que va detrás de las opciones y que nos permite seleccionar los paquetes que estamos buscando. En ausencia de ésta, el Tcpdump volcará todo el tráfico que vea el adaptador de red seleccionado.

  Tcpdump es considerado como el sniffer clásico para monitoreo de redes y adquisición de información.

  Entre los usos más comunes que se le dan a esta herramienta se encuentran:

a. Para depurar aplicaciones que utilizan la red para comunicar.

b. Para depurar la red misma.

c. Para capturar y leer datos enviados por otros usuarios o computadores. Algunos protocolos como Telnet y HTTP no cifran los datos que envían en la red. Un usuario que tiene el control de un router a través del cual circula tráfico no cifrado puede usar Tcpdump para lograr contraseñas u otras informaciones.

Esta herramienta puede ser descargada del sitito oficial <http://www.tcpdump.org/>

- **Snort.** Es un sniffer de paquetes y un detector de intrusos basado en red. Es un software muy flexible que ofrece capacidades de almacenamiento de sus bitácoras tanto en archivos de texto como en bases de datos abiertas como lo es MySQL. Implementa un motor de detección de ataques y barrido de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente definida.

  Este IDS implementa un lenguaje de creación de reglas flexibles, potentes y sencillas.

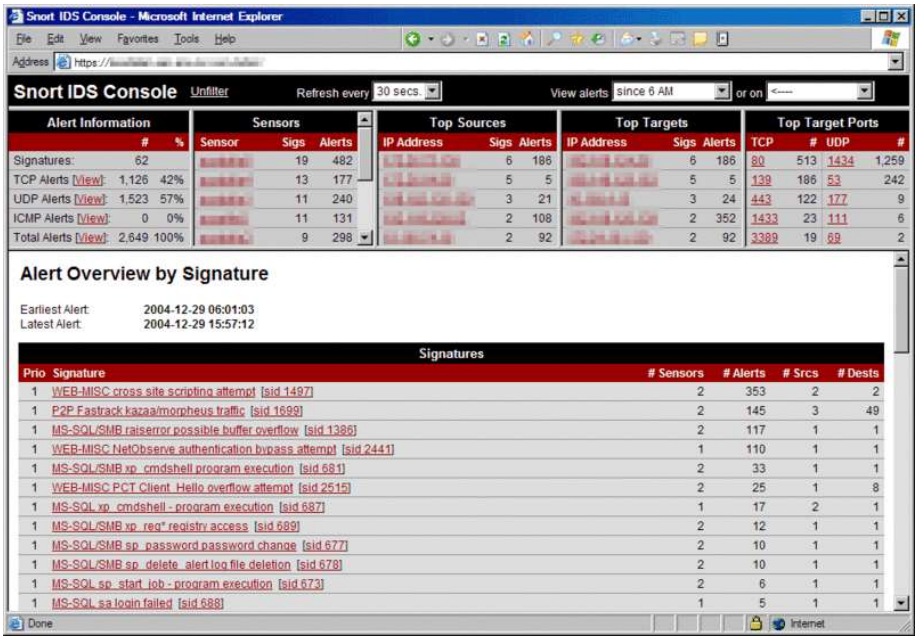
  Puede funcionar como sniffer (podemos ver en consola y en tiempo real qué ocurre en nuestra red, todo nuestro tráfico), registro de paquetes (permite guardar en un archivo los logs para su posterior análisis, un análisis offline) o como un IDS normal (en este caso NIDS). Cuando un paquete coincide con algún patrón establecido en las reglas de configuración, se loguea. Así se sabe cuando, de donde y cómo se produjo el ataque.

Snort está disponible bajo licencia GPL, gratuito y funciona bajo plataformas Windows y UNIX/Linux. Dispone de una gran cantidad de filtros o patrones ya predefinidos, así como actualizaciones constantes ante casos de ataques, barridos o vulnerabilidades que vayan siendo detectadas a través de los distintos boletines de seguridad.

La característica más apreciada de Snort, además de su funcionalidad, es su subsistema flexible de firmas de ataques. Snort tiene una base de datos de ataques que se está actualizando constantemente y a la cual se puede añadir o actualizar a través de la Internet. Los usuarios pueden crear 'firmas' basadas en las características de los nuevos ataques de red y enviarlas a la lista de correo de firmas de Snort, para que así todos los usuarios de Snort se puedan beneficiar. Esta ética de comunidad y compartir ha convertido a Snort en uno de los IDSes basados en red más populares, actualizados y robustos.

Esta herramienta puede ser descargada del sitito oficial <http://www.snort.org/> En la Figura No. 20 se muestra un ejemplo de captura de la consola del sistema.

Figura 20. Captura de la consola del sistema de Snort.



Fuente: Wikipedia, La enciclopedia libre, *SNORT*. [en línea]. [Fecha de consulta; 3 de Abril de 2007]. Disponible en: <http://es.wikipedia.org/wiki/Snort>

- **Ettercap**. Es un interceptor/sniffer/registrador para LANs con switch. Soporta disecciones activas y pasivas de varios protocolos (incluso aquellos cifrados, como SSH y HTTPS). También hace posible la inyección de datos en una conexión establecida y filtrado al vuelo aun manteniendo la conexión sincronizada gracias a su poder para establecer un Ataque Man-in-the-middle (Spoofing). Muchos modos de sniffing fueron implementados para darnos un conjunto de herramientas poderoso y completo de sniffing. (Ver Figura No. 21)

  Entre las funciones primordiales de esta herramienta se destacan:

  a. Inyección de caracteres en una conexión establecida emulando comandos o respuestas mientras la conexión está activa.

b. Compatibilidad con SSH1: puede interceptar users y passwords incluso en conexiones "seguras" con SSH.

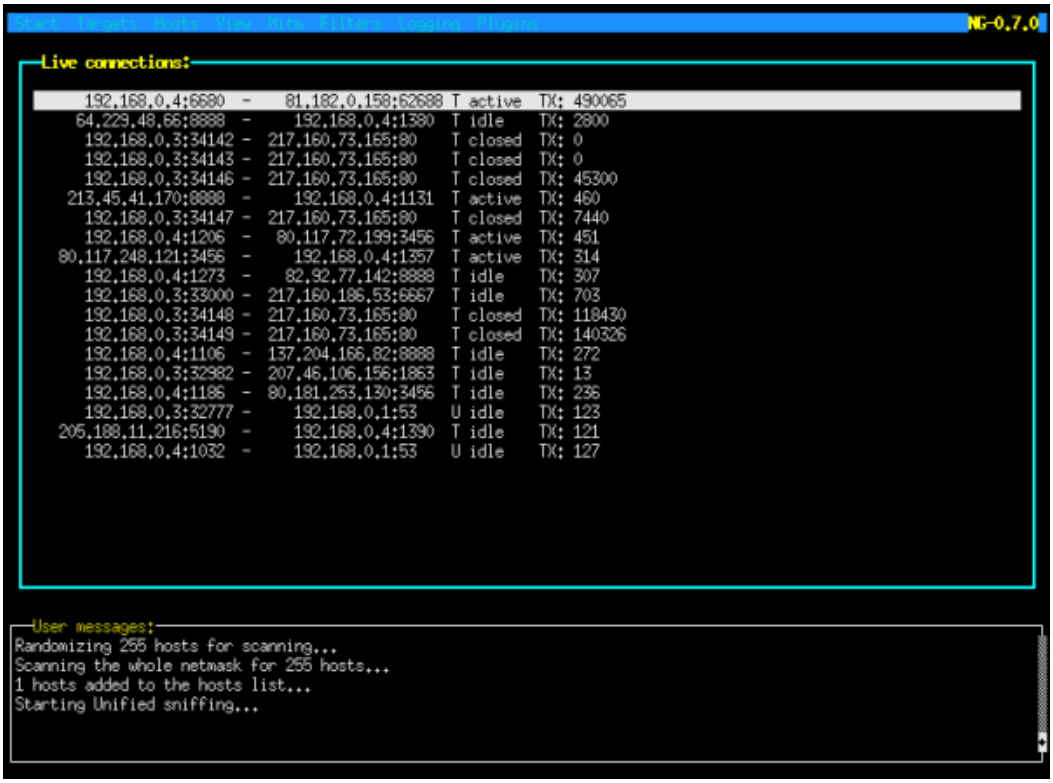
c. Compatibilidad con HTTPS: intercepta conexiones mediante http SSL (supuestamente seguras) incluso si se establecen a través de un proxy.

d. Intercepta tráfico remoto mediante un túnel GRE: si la conexión se establece mediante un túnel GRE con un router Cisco, puede interceptarla y crear un ataque "Man in the Middle".

e. "Man in the Middle" contra túneles PPTP (Point-to-Point Tunneling Protocol).

Esta herramienta puede ser descargada del sitito oficial <http://ettercap.sourceforge.net/>

Figura 21. Funcionamiento de Ettercap.



Fuente. Freshmeat. Ettercap - Next Generation branch. [en línea]. [Fecha de consulta; 5 de Abril de 2007] Disponible en: <http://freshmeat.net/projects/ettercap/>

- **Wireshark.** Es un sniffer anteriormente conocido como Ethereal. Wireshark es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones para desarrollo de software y protocolos, y como una herramienta didáctica para educación. Cuenta con todas las características estándar de un analizador de protocolos.

  La funcionalidad que provee es similar a la de Tcpdump, pero añade una interfaz gráfica y muchas opciones de organización y filtrado de información. Así, permite ver todo el tráfico que pasa a través de una red (usualmente una

red Ethernet, aunque es compatible con algunas otras) estableciendo la configuración en modo promiscuo. También incluye una versión basada en texto llamada tshark.

Permite examinar datos de una red viva o de un archivo de captura salvado en disco. Se puede analizar la información capturada, a través de los detalles y sumarios por cada paquete. Wireshark incluye un completo lenguaje para filtrar lo que queremos ver y la habilidad de mostrar el flujo reconstruido de una sesión de TCP.

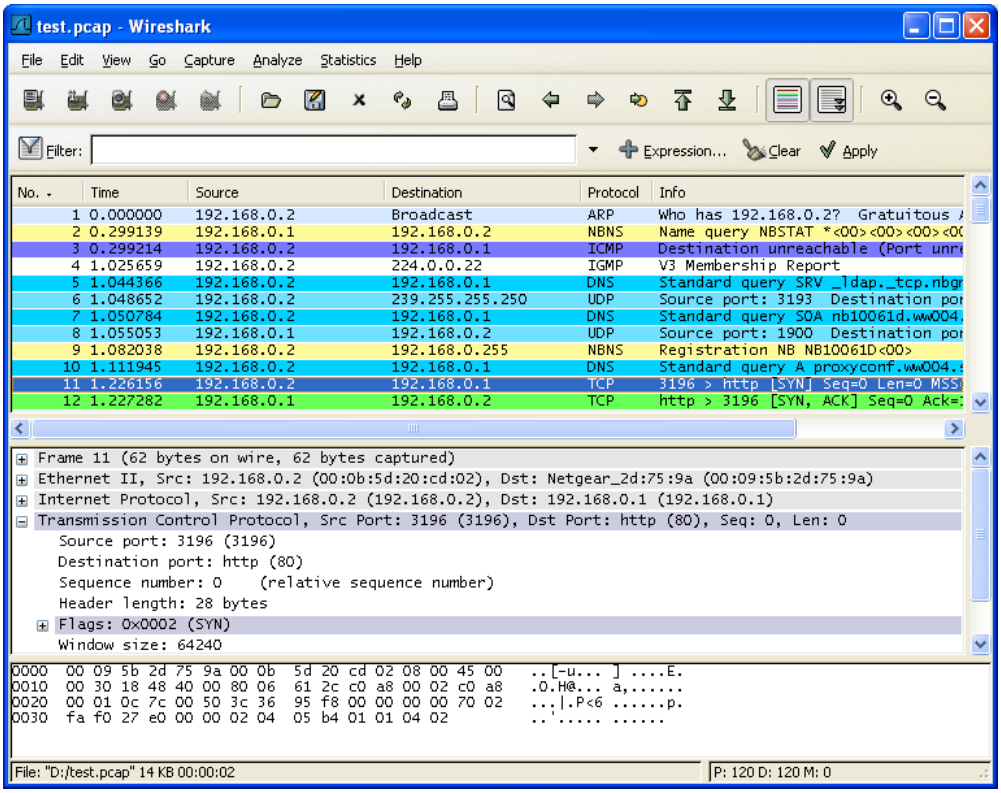
Wireshark es software libre, y se ejecuta sobre la mayoría de sistemas operativos Unix y compatibles, incluyendo Linux, Solaris, FreeBSD, NetBSD, OpenBSD, y Mac OS X, así como en Microsoft Windows. (Ver figura No. 22)

Esta herramienta se caracteriza por:

a. Estar mantenida bajo la licencia GPL.
b. Trabajar tanto en modo promiscuo como en modo no promiscuo.
c. Poder capturar datos de la red o leer datos almacenados en un archivo (de una captura previa).
d. Basarse en la librería pcacp.
e. Tener una interfaz muy flexible.
f. Tener capacidades de filtrado muy ricas.
g. Admitir el formato estándar de archivos tcpdump.
h. Reconstruir sesiones TCP.
i. Ejecutarse en más de 20 plataformas.
j. Ser compatible con más de 480 protocolos.

Esta herramienta puede ser descargada del sitito oficial <http://www.wireshark.org/>

Figura 22. Funcionamiento de Wireshark.



Fuente: Wireshark. Installing Wireshark under Windows. [en línea]. [Fecha de consulta; 5 de Abril de 2007] Disponible en: <http://www.wireshark.org/docs/wsug_html/>

2.2.2 Firewalls

– **Netfilter/IPtables.** Netfilter es el nombre que recibe el proyecto que se encarga de ofrecer herramientas libres para cortafuegos basados en Linux.

El componente más popular construido sobre Netfilter (framework) es Iptables, una herramienta de cortafuegos que permite no solamente filtrar paquetes, sino también realizar traducción de direcciones de red (NAT) para IPv4 o mantener registros de Log. A grandes rasgos, Iptables es el nombre de la herramienta de

espacio de usuario mediante la cual el administrador de la red puede definir políticas de filtrado del tráfico que circula por la misma.

Iptables es un conjunto de herramientas (comandos) que le permiten al usuario enviar mensajes al kernel del Sistema operativo. El kernel tiene todo el manejo de paquetes TCP/IP metido dentro de él, no es algo aparte como lo es en otros sistemas operativos, por lo tanto todos los paquetes que van destinados a un Linux o lo atraviesan son manejados por el mismo kernel.

Entonces, Iptables es una forma de indicarle al kernel algunas cosas que debe hacer con cada paquete, esto se hace en base a las características de un paquete en particular. Los paquetes de red tienen muchas características, algunas pueden ser los valores que tienen en sus encabezados (a donde se dirigen, de donde vienen, números de puertos, etc., etc.), otra puede ser el contenido de dicho paquete (la parte de datos), y existen otras características que no tienen que ver con un paquete en particular sino con una sumatoria de ellos. La idea es lograr identificar un paquete y hacer algo con el mismo.

Resumiendo brevemente que es Iptables, se dice que es un aplicativo del espacio de usuario que le permite a un administrador de sistema configurar las tablas, cadenas y reglas de Netfilter. Debido a que Iptables requiere privilegios elevados para operar, el único que puede ejecutarlo es el superusuario. En la mayoría de los sistemas Linux, Iptables está instalado como /sbin/iptables.

Modo de operación de Iptables

Iptables permite al administrador del sistema definir reglas acerca de qué hacer con los paquetes de red. Las reglas se agrupan en cadenas**:** cada cadena es una lista ordenada de reglas. Las cadenas se agrupan en tablas**:** cada tabla está asociada con un tipo diferente de procesamiento de paquetes.

Cada regla especifica qué paquetes la cumplen (match) y un destino que indica qué hacer con el paquete si éste cumple la regla. Cada paquete de red que llega a un computador o que se envía desde otro recorre por lo menos una cadena y cada regla de esa cadena se comprueba con el paquete. Si la regla cumple con el datagrama, el recorrido se detiene y el destino de la regla dicta lo que se debe hacer con el paquete. Si el paquete alcanza el fin de una cadena predefinida sin haberse correspondido con ninguna regla de la cadena, la política de destino de la cadena dicta qué hacer con el paquete. Si el paquete alcanza el fin de una cadena definida por el usuario sin haber cumplido ninguna regla de la cadena o si la cadena definida por el usuario está vacía, el recorrido continúa en la cadena que hizo la llamada (lo que se nombra *implicit target RETURN* o RETORNO de destino implícito). Solo las cadenas predefinidas tienen políticas.

En Iptables, las reglas se agrupan en cadenas. Una cadena es un conjunto de reglas para paquetes IP, que determinan lo que se debe hacer con ellos. Cada regla puede desechar el paquete de la cadena (cortocircuito), con lo cual otras cadenas no serán consideradas. Una cadena puede contener un enlace a otra cadena: si el paquete pasa a través de esa cadena entera o si cumple una regla de destino de retorno, va a continuar en la primera cadena. No hay un limite respecto de cuán anidadas pueden estar las cadenas. Hay tres cadenas básicas (*INPUT*, *OUTPUT* y *FORWARD*: ENTRADA, SALIDA y REENVÍO) y el usuario puede crear tantas como desee. Una regla puede ser simplemente un puntero a una cadena.

2.2.3 Antivirus

- **ClamAV.** Clam Antivirus es un conjunto de herramientas GPL anti-virus para UNIX. El principal objetivo de este software es la integración con servidores de

correo (análisis de adjuntos). El paquete dispone de un demonio multi-hilo flexible y escalable, un escáner de línea de comando, y una herramienta para actualización automática a través de Internet. Los programas se basan en una librería compartida distribuida con el paquete de Clam AntiVirus, que puede utilizar con su software. Aun más importante, la base de datos de virus se mantiene actualizada.

Algunas de sus características principales son:

a. Escáner de línea de comandos.
b. Rápido demonio multi-hilo.
c. Interfaz milter para sendmail.
d. Actualizador de base de datos con soporte para firmas digitales.
e. Librería de C de análisis de virus.
f. Análisis según acceso (Linux y FreeBSD).
g. Múltiples actualizaciones diarias de la base de datos de virus (ver la página principal para el número total de firmas).
h. Soporte embebido para RAR (2.0), Zip, Gzip, Bzip2, Tar, MS OLE2, MS Cabinet files, MS CHM (HTML Comprimido), MS SZDD.
i. Soporte embebido para mbox, Maildir, y archivos de correo en formato raw.
j. Soporte embebido para archivos Portable Executable comprimidos con UPX, FSG, y Petite.

- **Bitdefender.** Provee soluciones de seguridad para satisfacer los requisitos de protección del entorno informático actual, brindando una efectiva gestión de amenazas informáticas a unos 41 millones de usuarios domésticos y corporativos en más de 200 países.

a. Ofrece protección antivirus, cortafuego, antispyware y control parental a usuarios domésticos y corporativos.

b. La gama de productos BitDefender está desarrollada para implementarse en estructuras TI complejas (estaciones de trabajo, servidores de archivos, servidores de correos y puertas de enlace) en plataformas Windows, Linux y FreeBSD.

c. Distribución a nivel mundial, productos disponibles en 18 idiomas.

d. Fácil de usar, con un asistente de instalación que guía a los usuarios a través del proceso de instalación y realiza pocas preguntas.

e. Productos certificados a nivel internacional: Virus Bulletin, ICSA Labs, Checkmark, IST Prize, etc.

f. Atención al cliente continua - el equipo de atención al cliente está disponible 24 horas al día, 7 días a la semana.

g. Tiempo de respuesta rápido como un rayo ante los ataques a ordenadores nuevos.

h. El mejor radio de detección.

i. Actualizaciones de las firmas de virus cada hora - acciones automáticas o programadas que le ofrecen protección ante los nuevos virus.

- **Sophos.** Sophos Endpoint Security and Control proporciona protección integrada contra virus y programas espía de diferentes plataformas en servidores, ordenadores y portátiles, que no sean Windows. El poderoso motor de detección escanea todos los puntos posibles de entrada para una protección total de la red.

a. *Detección y limpieza con protección antivirus galardonada.* Detección y desinfección de virus, programas espía, troyanos y gusanos en tiempo real y en todos los puntos susceptibles de infección, para garantizar la protección total de la red en plataformas como NetWare y la mayoría de versiones de UNIX. Sophos Anti-Virus está certificado Checkmark 100% para la detección de programa espía.

b. *Escaneado de alto rendimiento minimiza el gasto de recursos.* El escaneado y la desinfección pueden realizarse en demanda o de forma automática a intervalos programados, ocasionando un impacto mínimo en el rendimiento del sistema. La tecnología Decisión Caching™ acelera el escaneado y minimiza el impacto en el rendimiento del sistema al comprobar sólo los archivos nuevos o modificados.

c. *Detección de amenazas de día cero antes de su ejecución.* La exclusiva protección Behavioral Genotype® protege contra amenazas desconocidas, analizando comportamientos antes de que se ejecute el código, y ofrece las ventajas de un sistema de prevención contra intrusiones (HIPS).

d. *Actualizaciones mínimas y más rápidas.* Las actualizaciones más recientes de software y detección de virus se descargan de forma automática desde SophosLabs™, garantizando la protección total de todos los ordenadores de la red, incluidos los portátiles remotos.

e. *Informes automatizados y personalizados.* El administrador recibe informes sobre todos los incidentes víricos, facilitando aún más la administración diaria.

2.2.4 Proxies.

- **Squid.** Es un popular programa de software libre que implementa un servidor Proxy y un demonio para Web caché, publicado bajo licencia GPL. Tiene una amplia variedad de utilidades, desde acelerar un Servidor Web, guardando en caché peticiones repetidas a DNS y otras búsquedas para un grupo de gente que comparte recursos de la red, hasta caché de Web, además de añadir seguridad filtrando el tráfico. Está especialmente diseñado para ejecutarse bajo entornos tipo Unix.

  Squid ha sido desarrollado durante muchos años y se le considera muy completo y robusto. Soporta muchos protocolos, aunque se usa principalmente para HTTP y FTP.

  Squid posee las siguientes características:

  a. Proxy y Caché de HTTP, FTP, y otras URLs.
  b. Proxy para SSL.
  c. Jerarquías de Caché.
  d. ICP, HTCP, CARP, Caché Digests.
  e. Caché transparente.
  f. WCCP (Squid v2.3 y superior).
  g. Control de acceso.
  h. Aceleración de servidores HTTP.
  i. SNMP.
  j. Caché de resolución DNS.

2.2.5 Wrappers

- **Tcp wrappers.** El paquete Wrapper más ampliamente utilizado es el TCP-Wrappers, el cual es un conjunto de utilidades de distribución libre, escrito por Wietse Venema (co-autor de SATAN, con Dan Farmer, y considerado el padre de los sistemas Firewalls) en 1990.

  Consiste en un programa que es ejecutado cuando llega una petición a un puerto específico. Este, 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.

  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. Este tipo de comportamiento raya en la estrategia paranoica, ya vista cuando se definió la política de seguridad del firewall.

  Con lo mencionado hasta aquí, puede pensarse que los Wrappers son Firewall 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. Así, estos controles son el complemento perfecto de un Firewall y la instalación de uno no está supeditada a la del otro.

2.2.6 Criptografía

- **HTTPS.** El protocolo HTTPS es la versión segura del protocolo HTTP. El sistema HTTPS utiliza un cifrado basado en las Secure Socket Layers (SSL) para crear un canal cifrado (cuyo nivel de cifrado depende del servidor remoto y del navegador utilizado por el cliente) más apropiado para el tráfico de información sensible que el protocolo HTTP. Cabe mencionar que el uso del protocolo HTTPS no impide que se pueda utilizar HTTP. Es aquí, cuando nuestro navegador nos advertirá sobre la carga de elementos no seguros (HTTP), estando conectados a un entorno seguro (HTTPS).

  Los protocolos https son utilizados por navegadores como: Safari, Internet Explorer, Mozilla Firefox, Opera, entre otros.

  El puerto estándar para este protocolo es el 443.

- **SSH.** SSH (o Secure SHell) es el nombre de un protocolo y del programa que lo implementa, que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y que permite a los usuarios conectarse a un host remotamente. Permite manejar por completo la computadora mediante un intérprete de comandos, y también puede redirigir el tráfico de X para poder ejecutar programas gráficos si tenemos un Servidor X arrancado. Además de la conexión a otras máquinas, SSH nos permite copiar datos de forma segura (tanto archivos sueltos como simular sesiones FTP cifradas), gestionar claves RSA para no escribir claves al conectar a las máquinas y pasar los datos de cualquier otra aplicación por un canal seguro tunelizado mediante SSH.

A diferencia de otros protocolos de comunicación remota tales como FTP o Telnet, SSH encripta la sesión de conexión, haciendo imposible que alguien pueda obtener contraseñas no encriptadas.

SSH está diseñado para reemplazar los métodos más viejos y menos seguros para registrarse remotamente en otro sistema a través de la shell de comando, tales como Telnet o rsh. Un programa relacionado, el scp, reemplaza otros programas diseñados para copiar archivos entre hosts como rcp. Ya que estas aplicaciones antiguas no encriptan contraseñas entre el cliente y el servidor, evite usarlas mientras le sea posible. El uso de métodos seguros para registrarse remotamente a otros sistemas reduce los riesgos de seguridad tanto para el sistema cliente como para el sistema remoto.

El protocolo SSH proporciona los siguientes tipos de protección:

a. Después de la conexión inicial, el cliente puede verificar que se está conectando al mismo servidor al que se conectó anteriormente.

b. El cliente transmite su información de autenticación al servidor usando una encriptación robusta de 128 bits.

c. Todos los datos enviados y recibidos durante la sesión se transfieren por medio de encriptación de 128 bits, lo cual los hacen extremamente difícil de descifrar y leer.

d. El cliente tiene la posibilidad de reenviar aplicaciones X11 desde el servidor. Esta técnica, llamada reenvío por X11, proporciona un medio seguro para usar aplicaciones gráficas sobre una red.

2.3 PRUEBAS DE INTRUSIÓN REALIZADAS SOBRE LA RED LAN DE LA UNIVERSIDAD AUTÓNOMA DE BUCARAMANGA

Los resultados obtenidos en estas pruebas es información confidencial ya que ésta compromete la seguridad de la red LAN de la Universidad Autónoma de Bucaramanga – UNAB y a la cual solo tendrá acceso el personal del Departamento de Tecnologías de Información y Comunicaciones de la UNAB.

A continuación se describe de modo general las pruebas realizadas en la red LAN de la UNAB

2.3.1 Escaneo en busca de posibles vulnerabilidades. En estas pruebas se emplearon herramientas de software libre utilizadas para realizar escaneos sobre el segmento de la red LAN de la Universidad Autónoma de Bucaramanga, donde se encuentran implementados los servidores de dicha institución, con el propósito de detectar posibles vulnerabilidades que puedan ser explotadas por personal no autorizado para efectuar ataques e intrusiones con fines delictivos y/o destructivos.

Algunas de las herramientas que se emplearon para conseguir dicho objetivo fueron: Nmap, LANguard, VNC, Nessus y LCP.

2.3.2 Intrusión a algunos de los servidores y equipos de la red LAN de la Universidad Autónoma de Bucaramanga. En esta sección se describirá de qué manera se accedió a algunos de los servidores y equipos de los cuales dispone la Universidad Autónoma de Bucaramanga, por medio de las vulnerabilidades previamente estudiadas y detectadas en los mismos.

Dichas vulnerabilidades encontradas en los servidores y equipos dan paso a la realización de ataques o siniestros que atentan contra los objetivos básicos de la seguridad informática (confidencialidad, integridad y disponibilidad de la información) de cualquier organización. Es por ésto que es de importancia conocer las herramientas y métodos empleados para efectuar dichos siniestros, y de igual forma, conocer las herramientas y métodos disponibles para prevenir, detectar y contrarrestar dichos ataques.

En el desarrollo de este punto se expuso el conjunto de pruebas realizadas sobre la LAN de la Universidad Autónoma de Bucaramanga de manera detallada, sencilla e ilustrativa, a fin de mostrar algunas debilidades halladas en la gestión de su seguridad informática.

2.4 RECOMENDACIONES SOBRE SEGURIDAD INFOMÁTICA

En esta sección del documento, se plantean algunas recomendaciones generales de seguridad que pueden ser útiles para los administradores de la red LAN de la Universidad Autónoma de Bucaramanga, a fin de tratar de limitar el número y alcance de incidentes presentados por fallos de seguridad informática. Estas recomendaciones no serán tratadas a un nivel detallado para no comprometer a la seguridad de la red LAN, por lo tanto se plantearán algunos aspectos generales que pueden ayudar a aumentar el nivel de seguridad de la red LAN de la UNAB con base en las debilidades encontradas.

2.4.1 Recomendaciones para el filtrado de paquetes. Aunque la seguridad a nivel del sistema sigue siendo de vital importancia, los fallos en varios servicios TCP/IP y la existencia de protocolos defectuosos hace imprescindible el uso de

filtros en el nivel de red, que permitan a una organización al restringir el acceso externo a estos servicios. De esta forma, sólo aquellos servicios que deban estar accesibles desde fuera del área local serán permitidos a través de filtros en los routers. Además es importante que estos filtros determinen las condiciones de acceso a los servicios permitidos.

Aunque es difícil implementar el filtrado correctamente, a continuación se dan algunos consejos que pueden resultar útiles para las organizaciones en el momento de implementar sus propios filtros en función a sus necesidades y a su topología de red concreta. En particular se sugiere que se filtren los siguientes servicios si no es necesario su acceso desde fuera de una organización concreta:

Tabla 3. Filtrado de Servicios.

Nombre	Puerto	Tipo de conexión	Servicio
echo	7	tcp/udp	Eco: Devuelve los datos que se reciben
systat	11	tcp	Información del sistema
netstat	15	tcp	Información sobre la red
chargen	19	tcp/udp	Generador de caracteres continuos.
SMTP	25	tcp	Puerto de correo
domain	53	tcp/udp	Servidor de Nombres (DNS)
bootp	67	udp	Arranque de estaciones remotas sin disco
tftp	69	udp	Arranque de equipos remotos, carga de configuraciones
link	87	udp	
supdup	95	udp	
sunrpc	111	tcp/udp	Servicio de RPC (portmapper)
news	119	tcp	Servidores de News
NetBios	137-139	udp/tcp	Servicios NetBios sobre TCP/IP (Windows)
snmp	161	udp	Gestión remota de equipos mediante SNMP

xdmpc	177	udp	Llegada de correo
exec	512	tcp	Ejecución remota de comandos (rexec)
login	513	tcp	Acceso remoto a un sistema (rlogin)
shell	514	tcp	Shell remoto
biff	512	udp	
who	513	udp	Información sobre los usuarios que hay conectados en un equipo remoto
syslog	514	udp	Almacenamiento de los logs de los sistemas en remoto
uucp	540	tcp	Envío de archivos y mensajes mediante uucp, actualmente en desuso
route	520	udp	Información sobre enrutamientos
openwin	2000	tcp	
NFS	2049	tcp/udp	Sistema de archivos remotos de Sun y Unix en general
X-Windows	6000 +n	tcp	Servidor X-Windows

Fuente: Autores del proyecto

En la tabla No. 3 se muestra la lista de servicios que deberían ser filtrados. En seguida se describirá brevemente la razón por la cual se debería tomar dicha medida.

a. ***Chargen y Echo:*** Puertos 11 y 19 (TCP/UDP). Es muy importante para evitar ataques de denegación de servicio por puertos UDP, filtrar a nivel de router o firewall los servicios "chargen" y "echo" y en general todos los servicios UDP que operen por debajo del puerto 900, con excepción de aquellos que se necesiten explícitamente.

b. ***Sistema de nombres de dominio (DNS):*** Puerto 53 (TCP/UDP). Es necesario filtrar el acceso desde el exterior a todos los equipos excepto a los servidores de DNS primarios y secundarios establecidos en una organización.

c. ***TFTP:*** Puerto 69 (UDP). En general cualquier servicio UDP que responde a un paquete de entrada puede ser víctima de un ataque de denegación de servicio (DoS).

   Un acceso no restringido al servicio TFTP permite a sitios remotos recuperar una copia de cualquier archivo "Word-readable", entre los que se pueden incluir archivos críticos como archivos de configuración de routers y archivos de claves. Es por ello, que aquellas organizaciones que no necesiten usar este servicio deberían filtrarlo y aquellas que necesiten usarlo, lo configuren adecuadamente teniendo en cuenta las medidas de seguridad a nivel de aplicación.

d. ***Comandos r de BSD UNIX:*** Puertos 512, 513 y 514 (TCP). Los comandos r incrementan el peligro de que sean interceptadas contraseñas en texto plano cuando se presenta un ataque utilizando sniffers de red, pero lo más importante es que son una fuente bastante frecuente de ataques y vulnerabilidades. Filtrando los puertos 512, 513 y 514 (TCP) en el hardware de red se evitará que personas ajenas a su organización puedan explotar estos comandos, pero no lo evitará a personas de su propia organización.

e. ***SunRPC y NFS:*** Puertos 111 y 2049 (TCP/UDP). Filtrar el tráfico NFS evitará que sitios ajenos a su organización accedan a sistemas de archivos exportados por máquinas de su red, pero como ocurría en el caso anterior, no se evitará que se realicen ataques desde dentro del área local. La mayoría de las implementaciones NFS emplean el protocolo UDP, por lo que es posible, en algunos casos, el envío de peticiones NFS falsificando la dirección origen de

los paquetes (IP-spoofing). Es por tanto muy aconsejable la instalación de las últimas versiones actualizadas de los servidores y clientes NFS que tienen en cuenta estas características.

f. ***SMTP:*** Puerto 25 (TCP). Es importante configurar el router de manera que todas las conexiones SMTP procedentes de fuera de una organización pasen a una oficina central y que sea desde ésta, donde se distribuya el correo internamente. Este tipo de filtros permitirá que no existan puertos 25 descontrolados dentro de una organización, ya que suelen ser foco de importantes problemas de seguridad, además de un registro centralizado de información, que podrá ayudar a la hora de detectar el origen de intentos de ataque. El administrador del sistema o el responsable de seguridad sólo se tendrá que preocupar de tener actualizado este servidor para evitar ataques aprovechando vulnerabilidades o fallos bien conocidos en los mismos

g. ***NetBios:*** Puertos 137, 138 y 139 (TCP/UDP). Estos puertos son los empleados en las redes Microsoft (Windows para Trabajo en Grupo, dominios NT, y LANManager), tanto para la autenticación de usuarios como para compartir recursos. Es frecuente el permitir el acceso global a uno de estos dispositivos, ignorando que es posible el acceso a estos recursos desde cualquier dirección de Internet.

h. ***SNMP:*** Puerto 161 (UDP/TCP). Muchos equipos disponen en la actualidad de gestión SNMP incorporada. Dado que estas facilidades de gestión no suelen necesitar accesos externos, se deben establecer filtros a nivel de router que eviten que se pueda obtener información sobre los dispositivos (routers, hubs, switches) desde el exterior o incluso se gestionen los equipos en remoto.

i. ***Filtros de datagramas IP:*** Por otro lado, para prevenir los ataques basados en bombas ICMP, se deben filtrar los paquetes de redirección ICMP y los

paquetes de destino ICMP inalcanzables. Además, y dado que actualmente el campo de opciones de los paquetes IP apenas se utiliza, se pueden filtrar en la totalidad de las organizaciones los paquetes de origen enrutado (source routed packets). Estos paquetes indican el camino de vuelta que ha de seguir el paquete, lo cual es algo inseguro, ya que alguno de los puntos intermedios por los que pase el paquete puede estar comprometido.

2.4.2 Recomendaciones para la administración de contraseñas. Una contraseña o clave, es una forma de autenticación (mediante la verificación de la identidad del usuario) que utiliza información secreta para controlar el acceso hacia algún recurso.

El uso de contraseñas permite escalar o no privilegios. Es decir, aquellos usuarios que desean acceder a la información se les solicita una clave; si conocen o no conocen la contraseña, se concede o se niega el acceso a la información según sea el caso.

Para propósitos de seguridad en sistemas de información, se recomienda usar contraseñas que acepten o nieguen el acceso al mismo de acuerdo a la jerarquía de privilegios designados dentro de las organizaciones. Para el cumplimiento de tal objetivo, existen diferentes pautas para la creación de contraseñas seguras y/o robustas, y del mismo modo, existen consejos prácticos para manejar dichas contraseñas dentro de los sistemas de información.

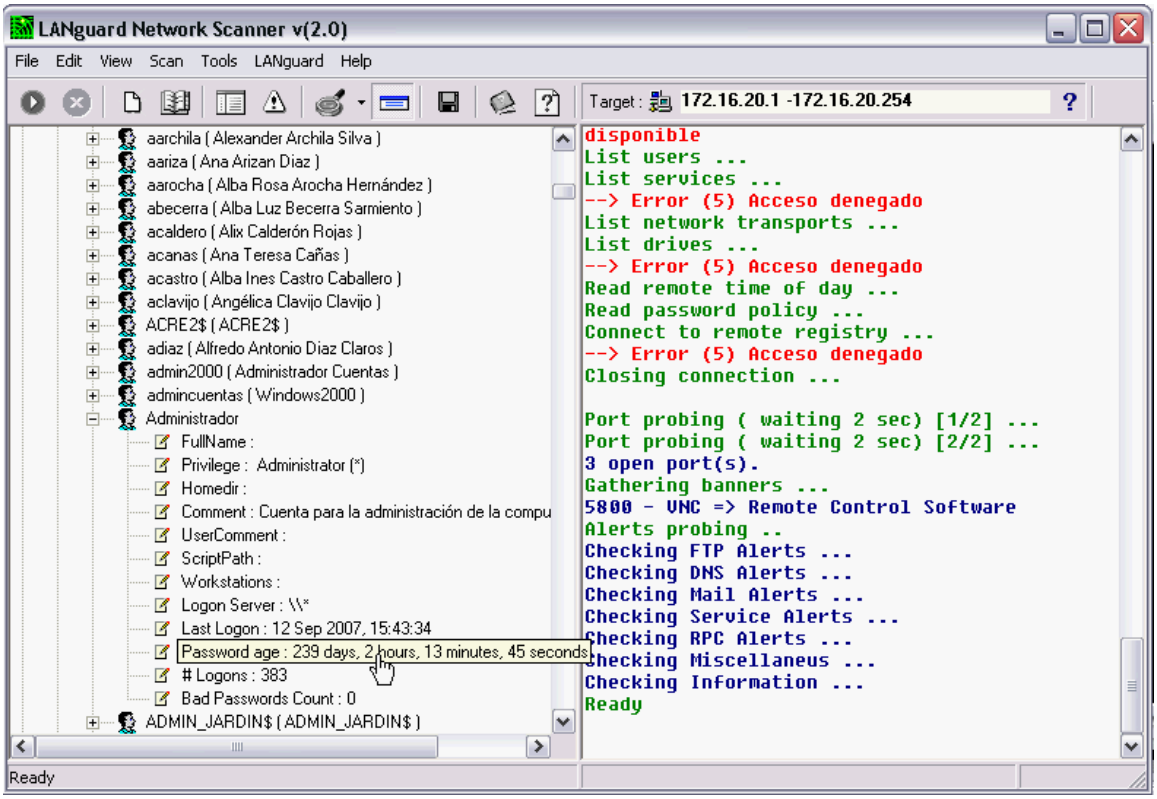
En primera instancia, recomendar o forzar a los usuarios a que cambien sus contraseñas frecuentemente (ya sea semestralmente, mensualmente o en lapsos más frecuentes) asegura que una contraseña válida en manos equivocadas sea eventualmente inútil.

Los beneficios de seguridad son limitados debido a que los atacantes frecuentemente sacan provecho de una contraseña tan pronto como ésta es revelada. En muchos casos, particularmente con las cuentas de administradores o cuentas "raíz", una vez que un hacker ha ganado acceso, puede realizar alteraciones al sistema operativo que le permitirán accesos futuros incluso si la contraseña inicial ya ha expirado.

Un ejemplo claro de la no aplicación de esta política en la Universidad Autónoma de Bucaramanga, pudo ser vista en el servidor ZEUS (Figura No. 23), donde se apreció que para una cuenta de Usuario Administrador, la contraseña no se había renovado en mas de 239 días, haciendo que usuarios malintencionados, apoyados en herramientas y técnicas de hacking, pudieran obtenerla para fines delictivos.

Es por tanto, que se sugiere cambiar las contraseñas de acceso tanto a servidores como a máquinas independientes regularmente, a fin de despistar a los delincuentes y a usuarios malintencionados. De acuerdo al nivel de seguridad de la contraseña establecida, se determinará el tiempo de vigencia de ésta. Una contraseña que tenga menos de 8 caracteres no debe mantenerse durante un período superior a una semana, mientras que una contraseña de 14 caracteres o más (y que cumpla un conjunto de normas indicadas a continuación para la creación de contraseñas) puede mantenerse sin problemas durante mayor cantidad de tiempo.

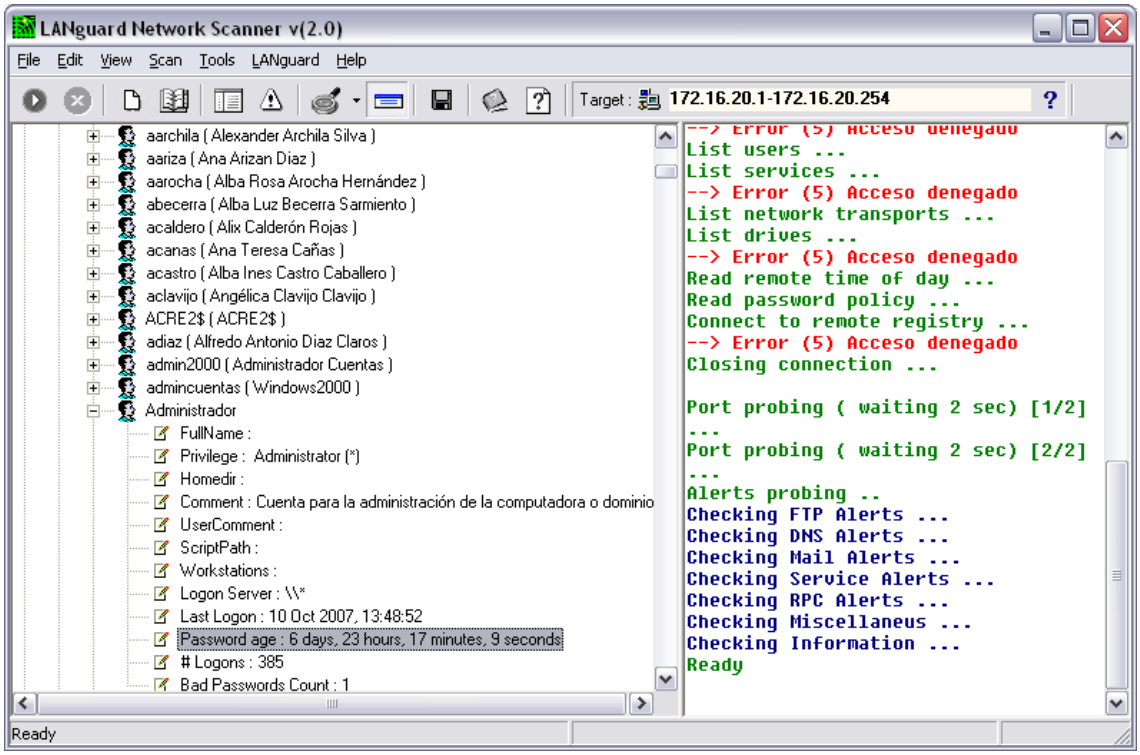
Figura 23. Tiempo de Uso de la contraseña para Administrador en el servidor ZEUS.



Fuente: Autores del proyecto

En el caso UNAB, se puede ver que ya se están empezando a tomar medidas al respecto, y se están aplicando políticas de este tipo (renovación de contraseñas), a fin de reducir el riesgo de ataques a la red LAN, basados en las vulnerabilidades detectadas. En la Figura No. 24, se muestra la misma cuenta de Administrador con una contraseña renovada actualmente.

Figura 24. Tiempo de Uso de una contraseña renovada para Administrador en el servidor ZEUS.



Fuente: Autores del proyecto

En segunda instancia, se recomienda a todos los usuarios de la red, crear contraseñas robustas y seguras, teniendo en cuenta las siguientes pautas básicas.

– **Recomendaciones para no crear contraseñas inseguras**

a. Utilice contraseñas que incluyan caracteres y números. Nunca utilice únicamente letras o sólo números en una contraseña.

Algunos ejemplos inseguros incluyen:

- 8675309
- Juan

b. No utilice palabras reconocibles. Palabras tales como nombres propios, palabras del diccionario o hasta términos de shows de televisión o novelas deberían ser evitados, aún si estos son terminados con números.

   Algunos ejemplos inseguros incluyen:

   - casa
   - Jennifer
   - smallville

c. No utilice palabras en idiomas extranjeros. Los programas de descifrado de contraseñas a menudo verifican contra listas de palabras que abarcan diccionarios de muchos idiomas. No es seguro confiarse en un idioma extranjero para asegurar una contraseña.

   Algunos ejemplos inseguros incluyen:

   - cheguevara
   - bienvenue1
   - 1dumbKopf

d. No utilice terminología de hackers.

   Algunos ejemplos inseguros incluyen:

   - H4X0R
   - 1337

e. No utilice información personal. Manténgase alejado de la información personal. Si un atacante conoce quién es usted, la tarea de deducir su contraseña será aún más fácil. La lista siguiente muestra los tipos de información que debería evitar cuando esté creando una contraseña:

Algunos ejemplos inseguros incluyen:

- Su nombre
- El nombre de sus mascotas
- El nombre de los miembros de su familia
- Fechas de cumpleaños
- Su número telefónico o código postal

f. No invierta palabras reconocibles. Los buenos verificadores de contraseñas siempre invierten las palabras comunes, por tanto invertir una mala contraseña no la hace para nada más segura.

Algunos ejemplos inseguros incluyen:

- R0X4H
- tagobo
- 9-DS

g. No escriba su contraseña. Nunca guarde su contraseña en un papel. Es mucho más seguro memorizarla.

h. No utilice la misma contraseña para todas las máquinas. Es importante que tenga contraseñas separadas para cada máquina. De esta forma, si un sistema es comprometido, no todas sus máquinas estarán en peligro inmediato.

– **Recomendaciones para crear contraseñas seguras**

a. Cree contraseñas de al menos ocho caracteres. Mientras más larga sea la contraseña, mejor.

b. Mezcle letras mayúsculas y minúsculas.

c. Mezcle letras y números. Agregando números a las contraseñas, especialmente cuando se añaden en el medio (no solamente al comienzo o al final), puede mejorar la fortaleza de su contraseña.

d. Incluya caracteres no alfanuméricos. Los caracteres especiales tales como &, $, y > pueden mejorar considerablemente su contraseña.

e. Seleccione una contraseña que pueda recordar. La mejor contraseña en el mundo será de poca utilidad si usted no puede recordarla. Por lo tanto utilice acrónimos u otros dispositivos nemónicos que lo ayuden a memorizar las contraseñas.

De igual manera, siga los pasos descritos por la metodología que se mostrará a continuación para crear contraseñas seguras:

a. Piense en una frase que pueda recordar. Ésta será la base de su contraseña segura o frase codificada. Piense en una frase que pueda memorizar sin problemas, como "Mi hijo Ángel tiene tres años".

b. Compruebe si el equipo o el sistema en línea admite directamente la frase codificada. Si puede utilizar una frase codificada (con espacios entre caracteres) en el equipo o en el sistema en línea, hágalo.

c. Si el equipo o el sistema en línea no admite frases codificadas, conviértalas en contraseñas. Utilice la primera letra de cada palabra de la frase que ha creado para definir una palabra nueva sin sentido. Si tomamos la frase del ejemplo anterior, tendríamos: "mhátta".

d. Aumente la complejidad combinando mayúsculas, minúsculas y números. También resulta de utilidad cambiar letras o cometer errores ortográficos

voluntariamente. Por ejemplo, en la anterior frase codificada, considere la posibilidad de escribir incorrectamente el nombre Ángel o de sustituir la palabra "tres" por el número 3. Existen muchas posibilidades de sustitución. Por otra parte, cuanto más larga sea la frase, más compleja podrá ser la contraseña. La frase codificada podría convertirse finalmente en "Mi Hijo Áng3l tiene 3 añiOs". Si el equipo o el sistema en línea no admite frases codificadas, utilice la misma técnica para la contraseña abreviada. El resultado podría ser una contraseña como "MhÁt3a".

e. Por último, realice sustituciones con algunos caracteres especiales. Puede utilizar símbolos que parezcan letras, combinar palabras (quitar espacios) y recurrir a otros medios que permitan crear contraseñas más complejas. Mediante estos trucos, podemos crear una frase codificada como "MiHiJo @ng3l ti3n3 3 añiO$" o una contraseña abreviada (con las primeras letras de cada palabra) como "MiHi@t3a".

2.4.3 Realizar actualizaciones constantes del software y el Sistema Operativo de los equipos de la UNAB. Mantener el software actualizado no es un capricho, una vez que es descubierta una vulnerabilidad en una versión de cualquier programa, todos los usuarios de ese software se vuelven vulnerables a ataques de seguridad que traten de sacar partido a ese error.

La solución sencilla y eficaz consiste en mantener actualizados los sistemas y equipos que se encuentren a disposición de estudiantes y el público en general debido que a partir de equipos dentro de la Universidad se podría empezar a escalar privilegios y llegar a un equipo verdaderamente importante que contenga información a la cual no se debería tener acceso.

2.4.4 Mensajería Instantánea. Los mensajes instantáneos por lo general no son encriptados y pueden ser interceptados fácilmente, spoofed o modificados usando distintas metodologías disponibles en los sitios de hackers de Internet.

2.4.5 Recomendaciones para el soporte Antispam de Sendmail. El correo spam, también conocido como correo comercial no solicitado o correo basura, es uno de los problemas mas importantes que acechan a Internet en estos tiempos. Principalmente el correo spam gasta dos grandes recursos de Internet: el ancho de banda usado para los enlaces de comunicaciones y el tiempo de los administradores de la red encargados de mantener Internet.

Enseguida se citan algunos métodos eficaces que hacen frente a los problemas presentados por el correo spam:

a. Eliminar de la lista blanca el dominio de la universidad, debido a que la lista Blanca es una lista de direcciones y dominios de correo de los cuales siempre desea recibir correo. Es decir, el correo enviado desde estas direcciones o dominios nunca será marcado como spam, por lo tanto se podrá enviar spam con el dominio de la universidad pasará por alto ya que este dominio se encuentra en la lista blanca.

b. Autenticar el demonio SMTP. El servidor de correo sendmail tiene dos opciones muy buenas tanto para la seguridad como para el control de acceso del servidor. Comúnmente se denominan como AUTH/STARTTLS.

    - Con soporte AUTH, sendmail requiere que todo el tráfico SMTP deba conectar con el servidor de correo con un nombre de usuario (login) y un password válidos. Para acceder a estas características es necesario instalar las librerías cyrus-sasl.

- Con soporte STARTTLS, todo el tráfico puede ir encriptado con SSL. Para soportar estas características es necesario instalar las librerías openssl.

c. Por último, instalando SpamAssassin, un filtro antispam que emplea todas las armas conocidas hasta el momento para luchar contra el correo no deseado.

2.4.6 Recomendaciones para evitar ser vulnerables ante XSS (Cross Site Scripting). Este fallo compromete más que nada, la seguridad del usuario y no la del servidor. Consiste en inyectar código HTML o Javascript en una aplicación Web, con el fin de que el navegador de un usuario ejecute el código inyectado al momento de ver la página alterada.

Comúnmente el XSS se utiliza para causar una acción indebida en el navegador de un usuario, pero dependiendo de la vulnerabilidad, puede explotarse el fallo para causar una acción indebida en un servidor o en una aplicación.

El XSS se puede utilizar para hacer phishing, robo de credenciales, troyanizar navegadores, o simplemente para hacer un deface. Todo depende de la página.

Existen tres tipos conocidos de vulnerabilidades XSS:

a. El tipo-0, que se utiliza para ejecutar código remotamente con los permisos de otro usuario.

b. El tipo-1, ataque no-persistente o reflejado (explicado más adelante) utilizado en páginas no estáticas.

c. El tipo-2, ataque persistente, donde se inyecta código en páginas estáticas.

El éxito de este ataque depende altamente de la ingeniería social aplicada por el atacante, debido a que éste debe enviar el link maligno a la víctima y es por ello que la gente suele ver el XSS como un ataque muy limitado.

3. CONCLUSIONES

En la actualidad gran número de entidades le están prestando mayor atención al tema de la seguridad informática, incrementando la cantidad de recursos destinados hacia este sector; puesto que de cierto modo, el valor de sus datos e información privada se han visto comprometidos debido a que usuarios no autorizados a los sistemas, se aprovechan de las vulnerabilidades y falencias que poseen las redes de datos para ejecutar acciones malintencionadas e ilegales.

Paralelamente al incremento de computadores en las redes LAN, aumenta la cantidad de amenazas y ataques a las mismas. Dicha situación evidencia la necesidad de buscar nuevas soluciones de seguridad informática, más transparentes y más flexibles que ayuden a conseguir los requisitos mínimos de seguridad para cualquier entidad.

Ninguna red de datos se considera 100% segura. Es por tanto que los administradores de la red no deberían confiarse de la seguridad con que cuentan actualmente, sino por el contrario, deberían valerse de técnicas y herramientas que atenten contra la seguridad informática de cualquier red, con el objeto de quebrantar sus medidas de seguridad implementadas, y de este modo, detectar y corregir sus falencias de manera preventiva, para lograr un mejor desempeño de la red.

Es recomendable que los administradores de la red tengan en cuenta algunos aspectos importantes como lo son: verificar y monitorear periódicamente el nivel

actual de la seguridad de su red, controlar el acceso a los datos e información para garantizar una comunicación autenticada, legítima y confidencial, y finalmente, pero no menos importante, diseñar, crear, implementar y difundir políticas de seguridad que ayuden a aminorar los posibles riesgos de seguridad antes los que una red está expuesta.

La realización y aplicación de la encuesta sobre seguridad en redes efectuada a diversas universidades de Bucaramanga, permitió identificar el nivel de seguridad con que cuenta cada institución, y del mismo modo, permitió obtener información acerca de las vulnerabilidades y ataques sufridos por dichas instituciones con sus respectivas medidas de seguridad acogidas para contrarrestar dichas falencias, con el objeto de establecer una base de conocimiento que sirva de referencia al momento de diagnosticar el estado actual de seguridad de la red LAN de la UNAB.

El spam, los virus, los troyanos y el sniffing, en su respectivo orden, son los ataques que con mayor incidentalidad se presentan como problema en las instituciones universitarias de Bucaramanga. Ante dicha situación, estas universidades se ven en la necesidad de implementar técnicas tales como: firewalls, proxies y antivirus, en orden de relevancia según los resultados de la encuesta realizada, a fin de prevenir y contrarrestar los ataques mencionados anteriormente.

La recopilación bibliográfica sobre los ataques más comunes que sufren las redes de datos de las universidades, se realizó con base en la previa aplicación de la encuesta sobre seguridad en redes, pues permitió distinguir y detectar los ataques más comunes, a fin de realizar su completa documentación.

Los sistemas operativos y el software empleado por los administradores de la red para gestionar la seguridad de la misma, deberían mantenerse al día en cuanto a actualizaciones disponibles se refiere, debido a que éstas ayudan a corregir fallos que han sido encontrados con anterioridad, y del mismo modo, evitan que las redes sean vulnerables a ataques realizados a través de la explotación de dichos fallos a equipos en la red que carecen de aquellas actualizaciones.

Se recomienda a los administradores de las redes y a los usuarios de equipos pertenecientes a cualquier red, renovar periódicamente las contraseñas de acceso a los sistemas, ya que esto aumenta la complejidad en el momento de que un atacante intente ingresar a cualquier sistema protegido por una contraseña.

Se recomienda incluir entre las políticas de seguridad de las organizaciones, que los usuarios finales no compartan recursos, en especial, no compartan carpetas, pues a través de ellas los atacantes podrán tener la posibilidad de extraer información confidencial y/o contraseñas de éstos equipos, hasta el punto de escalar privilegios y obtener la contraseña del Administrador, que consecuentemente podría conllevar a realizar otros tipos de ataque como producto del anterior.

Se recomienda a los administradores de la red habilitar únicamente los servicios de los cuales van a hacer uso, pues los maleantes se valen de las vulnerabilidades que éstos ofrecen para ejecutar ataques de diversa índole. Por ejemplo, un servidor que tenga abierto el puerto 23 (Telnet), podría ser accesible por un intruso a través del proceso de evasión de autenticación.

La recopilación, el análisis y la documentación de herramientas basadas en software libre para el escaneo y el ataque a las redes de datos, y en contraparte, el estudio de herramientas de software libre empleadas para detectar y contrarrestar los mismos, se realizó con el fin de adquirir conocimientos en la materia que permitieran efectuar las pruebas de seguridad pertinentes a la red de la UNAB.

Las pruebas de seguridad desarrolladas consistieron en la realización de un escaneo sobre segmentos de la red LAN. Este escaneo se efectuó a fin de detectar posibles vulnerabilidades presentes en la red para posteriormente evaluarlas y proponer correctivos de ser necesarios.

Las herramientas de software libre, tales como: LANguard, Nmap y Nessus, usadas en este proyecto, para escanear el segmento de red de los servidores y otros equipos con que cuenta la UNAB, permitió detectar algunas falencias de seguridad en las cuales se pueden explotar vulnerabilidades como: la vulnerabilidad de Telnet, la vulnerabilidad de RealVNC y la vulnerabilidad de RPC. Con estas pruebas realizadas quedó demostrado que la red LAN de esta institución presenta algunos problemas de seguridad que deben ser corregidos por los administradores de la seguridad informática.

Hoy en día, pese a que existen muchos métodos y herramientas para verificar el nivel de seguridad de las redes, se siguen presentando intrusiones no detectadas por el personal encargado de velar por la seguridad de la red. Esto significa, que los índices de ilegalidad informática son realmente altos, y lo más grave es que no se toman las medidas pertinentes para sancionar dichas acciones, ya sea porque la ley no aplica los correctivos necesarios, o porque los mismos administradores

no pueden determinar a ciencia cierta quien (es) cometieron las infracciones que atentan el bienestar de los usuarios de las redes.

BIBLIOGRAFÍA

ALVAREZ, Miguel Ángel. Que un Firewall. [en línea]. DesarrolloWeb.com. [Fecha de consulta: 27 de septiembre de 2007]. Disponible en <http://www.desarrolloweb.com/articulos/513.php>

BARRAGÁN Ortiz, Luz Ángela. Análisis de desempeño de software de detección de Vulnerabilidades como herramienta para implementar estudio de Seguridad computacional en redes locales. Bucaramanga, 2004. Maestría en informática (Ingeniera de sistemas). Universidad Industrial de Santander. Facultad de ingenierías físico-mecánicas.

BUSTOS, Pérez Jose Ángel. Criptografía. [en línea]. [Fecha de consulta: 28 de septiembre de 2007]. Disponible en <http://es.tldp.org/Presentaciones/200203jornadassalamanca/jadebustos/conferencia-criptografia.pdf>

CLAM ANTIVIRUS. About ClamAV [en línea]. [Fecha de consulta: 23 de octubre de 2007]. Disponible en: <http://www.clamav.org/about/>

CYSCOPRESS. Academia de Networking de Cisco Systems: Fundamentos de Seguridad de Redes Especialista en Firewall Cisco. Pearson. Madrid: Educación, S.A. 2005.

E. COLETTI, Daniel. Entendiendo Iptables. [en línea]. 27 de junio 2003 [Fecha de consulta: 23 de octubre de 2007]. Disponible en: <http://www.danielcoletti.com.ar/Documentos/Tech/Iptables/iptables/>

GFiLANguard. Network Security Scanner. Escáner de vulnerabilidad, gestión de parches y auditoria de red [en línea]. [Fecha de consulta: 12 de septiembre de 2007]. Disponible en: <http://www.gfihispana.com/es/lannetscan/>

GFiLANguard. Network Security Scanner. Escáner de vulnerabilidad, gestión de parches y auditoria de red [en línea]. [Fecha de consulta: 12 de septiembre de 2007]. Disponible en: <http://www.gfihispana.com/es/lannetscan/lanscanbrochure_es.pdf>

GURÚ de la informática. Escáner de redes gratuito, Nessus. [en línea]. [Fecha de consulta: 11 de septiembre de 2007].Disponible en: ttp://vtroger.blogspot.com/2007/05/escner-de-redes-de-gratuito-nessus.html>

HERNÁNDEZ, Roberto. Firewalls: Seguridad en las redes e Internet. Firewall. Segu-Info.Com.Ar, Seguridad de la Información. [en línea]. [Fecha de consulta: 27 de septiembre de 2007]. Disponible en <http://www.segu-info.com.ar/firewall/firewall.htm>

HISPASEC SISTEMAS. Detalles y evolución de la vulnerabilidad RPC/DNS de Microsoft Windows [en línea]. 17 de abril de 2007 [Fecha de consulta: 11 de septiembre de 2007]. Disponible en: <http://www.hispasec.com/unaaldia/3097>

HISPASEC Sistemas. Seguridad y tecnologías de la información. Grave Vulnerabilidad en RealVNC. Publicado el 15/05/2006. [en línea]. [Fecha de consulta: 10 de septiembre de 2007]. Disponible en <http://www.hispasec.com/unaaldia/2760>.

Informática Productiva Conocimiento y Tecnología. Antivirus – BitDefender [en línea]. [Fecha de consulta: 23 de octubre de 2007]. Disponible en: <http://www.puntoip.es/bitdefender/>

INGENIERÍA TÉCNICA INFORMÁTICA. Packet-sniffer (ettercap) [en línea]. Abril 17 de 2007 [Fecha de consulta: 3 de septiembre de 2007]. Disponible en: <http://euitio178.ccu.uniovi.es/wiki/index.php/Packet-sniffer>

INSECURE.Org. Guía de referencia de Nmap (Página de manual). [en línea]. [Fecha de consulta: 9 de septiembre de 2007]. Disponible en >http://insecure.org/nmap/man/es/index.html>

INSECURE.ORG. Las 75 Herramientas de Seguridad Más Usadas. [en línea]. [Fecha de consulta: 26 de febrero de 2007]. Disponible en: <http://insecure.org/tools/tools-es.html>

INTERLAN. Ingeniería de redes y sistemas LTDA. Evaluación de los Sistemas de Detección de Intrusos (IDS). Publicado el 30 de Septiembre del 2003. [en línea]. [Fecha de consulta: 26 de septiembre de 2007]. Disponible en <http://www.interlan.com.co/ids.htm >

INTERLAN. Ingeniería de Redes y Sistemas LTDA. GFiLANguard. Network Security Scanner. [en línea]. [Fecha de consulta: 12 de septiembre de 2007]Disponible en: <http://www.interlan.com.co/nss.htm>

INFOR SPYWARE. Firewall = Contrafuegos. Publicado el 20 de Septiembre del 2004 [en línea]. [Fecha de consulta: 27 de septiembre de 2007]. Disponible en <http://www.infospyware.com/Firewall/Cortafuegos.htm>

La Organización DragonJAR. LCP Una buena opción libre frente a l0phtcrack - Recuperación de contraseñas Windows. [en línea]. [Fecha de consulta: 20 de septiembre de 2007] Disponible en:<http://www.dragonjar.org/lcp-una-buena-opcion-libre-frente-a-l0phtcrack.xhtml>

LPCSoft [en línea]. [Fecha de consulta: 20 de septiembre de 2007]. Disponible en:<http://www.lcpsoft.com/english/index.htm#lcp>

MACHADO, Jorge. ¿Qué es un software Antivirus? [en línea]. [Fecha de consulta: 27 de septiembre de 2007]. Disponible en <http://www.perantivirus.com/sosvirus/pregunta/antiviru.htm>

MARTIN MARTÍN. Criterio y Funcionamiento de un Sniffer (Cain & Abel) [en línea]. [Fecha de consulta: 15 de marzo de 2007]. Disponible en: <http://www.informaticavip.com.ar>

MIRA, Alfonso. Sistemas de Detección de intrusos y Snort. [en línea]. Wordpress. Maestros del Web. [Fecha de consulta: 26 de septiembre de 2007] Disponible en <http://www.maestrosdelweb.com/editorial/snort/>

MURCIA, Camilo Ernesto. Introducción a Nmap [en línea]. 18 de agosto de 2003 [Fecha de consulta: 9 septiembre de 2007]. Disponible en: <http://www.maestrosdelweb.com/editorial/nmap/>

OVAL. Open Vulnerability and Assessments Language. About OVAL. [en línea]. 3 de enero de 2007 [fecha de consulta: 12 de septiembre de 2007]. Disponible en: <http://oval.mitre.org/oval/about/index.html>

Real VNC: The Original Cross Platform Remote Control Solution [en línea]. [Fecha de consulta: 9 de septiembre de 2007]. Disponible en: < http://www.realvnc.com/what.html>

Red Hat, Inc. Red Hat Enterprise Linux 4: Manual de seguridad. Capítulo 4: Intrusiones y respuestas a incidentes. [en línea]. [Fecha de consulta: 26 de septiembre de 2007]. Disponible en <http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/ch-detection.html>

Red Hat, Inc. Red Hat Enterprise Linux 4: Manual de seguridad. Capítulo 20: Protocolo SSH [en. [Fecha de consulta: 23 de octubre de 2007]. Disponible en: <http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/ch-ssh.html>

Red Hat, Inc. Red Hat Enterprise Linux 4: Manual de seguridad. IDS basados en host. [en línea]. [Fecha de consulta: 26 de septiembre de 2007]. Disponible en <http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/s1-ids-host.html>

Red Hat, Inc. Red Hat Enterprise Linux 4: Manual de seguridad. IDS basados en la red. [en línea]. [Fecha de consulta: 26 de septiembre de 2007]. Disponible en <http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/s1-ids-net.html>

RODRÍGUEZ SÁNCHEZ, Alfredo. Catálogo de herramientas [en línea]. Noviembre de 2006 [Fecha de consulta: 3 agosto de 2007]. Disponible en: <http://atc.inf-cr.uclm.es/docs/GdR/trabajos/Herramientas/Seguridad.doc>

SANS. About SANS. [en línea]. [Fecha de consulta: 1 de septiembre de 2007]. Disponible en: <http://www.sans.org/about/sans.php>

SEGURIDAD DIGITAL. Las 15 herramientas libres más utilizadas en hacking [en línea]. [Fecha de consulta: 20 de septiembre de 2007]. Disponible en:<http://www.seguridaddigital.info/index.php?option=com_content&task=view&id=128&Itemid=26>

SOPHOS. Proteja UNIX con Endpoint Security and Control [en línea]. [Fecha de consulta: 23 de octubre de 2007]. Disponible en: <http://esp.sophos.com/products/enterprise/endpoint/security-and-control/unix/index.html>

TARBOURIECH, Georges . Herramientas de Seguridad. [en línea]. [Fecha de consulta: 1 de septiembre de 2007].Disponible en <http://es.tldp.org/LinuxFocus/pub/mirror/LinuxFocus/Castellano/January2001/article180.shtml >.

TCP Wrappers. [en línea]. [Fecha de consulta: 27 de septiembre del 2007].Disponible en: <http://webdia.cem.itesm.mx/ac/rogomez/seguridad/tcpwrappers.html>

TELLA LLOP, Jose Manuel. SiquelNet, Vulnerabilidad y explotación del RPC [en línea]. [Fecha de consulta: 11 de septiembre de 2007]. Disponible en: <http://siquelnet.com/default.aspx?Tema=NET&Seccion=GENERAL&Articulo=010>

TENABLE Network Security. Nessus 3.0 Advanced User Guide. [en línea]. [Fecha de consulta: 12 de septiembre de 2007]. Disponible en: <http://www.nessus.org/documentation/nessus_3.0_advanced_user_guide.pdf>

TENABLE Network Security. Nessus 3.0 Client User Guide. [en línea]. [Fecha de consulta: 12 de septiembre de 2007]. Disponible en: <http://www.nessus.org/documentation/nessus_3.0_client_guide.pdf>

TENABLE Network Security. Nessus 3.0 Installation Guide. [en línea]. [Fecha de consulta: 12 de septiembre de 2007]. Disponible en: <http://www.nessus.org/documentation/nessus_3.0_advanced_user_ guide.pdf>

TEXTOS CIENTIFICOS.COM. RPC Llamada a procedimiento remoto [en línea]. [Fecha de consulta: 11 de septiembre de 2007]. Disponible en: <http://www.textoscientificos.com/redes/tcp-ip/servicios-capa-transporte/rpc>

THE WIL FAMILY. Nmap a fondo: Escaneo de redes y hosts. Junio 27, 2007. [en línea]. [Fecha de consulta: 9 de septiembre de 2007]. Disponible en <http://www.thewilfamily.com/hacking/nmap-a-fondo-escaneo-de-redes-y-hosts>

UNAB. Universidad Autónoma de Bucaramanga. Seguridad Informática. Octubre 17, 18 y 19 de 2002. Facultad de Ingeniería de Sistemas. IX Semana Técnica Internacional.

WIKIPEDIA, La enciclopedia libre. Antivirus [en línea]. [Fecha de consulta: 27 de septiembre de 2007]. Disponible en <http://es.wikipedia.org/w/index.php?title=Antivirus&oldid=12357804>

WIKIPEDIA, La enciclopedia libre. Bomba lógica [en línea]. [Fecha de consulta: 26 de septiembre de 2007]. Disponible en <http://es.wikipedia.org/w/index.php?title=Bomba_l%C3%B3gica&oldid=12350797>

WIKIPEDIA, La enciclopedia libre. Cortafuegos (informática) [en línea]. [Fecha de consulta: 21 de agosto de 2007]. Disponible en <http://es.wikipedia.org/w/index.php?title=Cortafuegos_%28inform%C3%A1tica%29&oldid=12374859>.

WIKIPEDIA, La enciclopedia libre. Criptografía [en línea]. [Fecha de consulta: 21 de agosto de 2007].Disponible en <http://es.wikipedia.org/w/index.php?title=Criptograf%C3%ADa&oldid=12053297>.

WIKIPEDIA, La enciclopedia libre. Ettercap. [en línea]. [Fecha de consulta: 22 de octubre de 2007]. Disponible en: <http://es.wikipedia.org/wiki/Ettercap>.

WIKIPEDIA, La enciclopedia libre. Exploit [en línea]. [Fecha de consulta: 12 de septiembre de 2007]. Disponible en <http://es.wikipedia.org/w/index.php?title=Exploit&oldid=12104607>.

WIKIPEDIA, La enciclopedia libre. Firma digital [en línea]. [Fecha de consulta: 21 de agosto de 2007].Disponible en <http://es.wikipedia.org/w/index.php?title=Firma_digital&oldid=12370246>.

WIKIPEDIA, La enciclopedia libre. Gusano informático [en línea]. [Fecha de consulta: 25 de septiembre de 2007]. Disponible en <http://es.wikipedia.org/w/index.php?title=Gusano_inform%C3%A1tico&oldid=12148416>.

WIKIPEDIA, La enciclopedia libre. HTTPS [en línea]. [Fecha de consulta: 23 de 2007]. Disponible en: <http://es.wikipedia.org/wiki/HTTPS>

WIKIPEDIA, La enciclopedia libre. Ingeniería social (seguridad informática) [en línea]. [Fecha de consulta: 17 de Agosto de 2007.]. Disponible en

<http://es.wikipedia.org/w/index.php?title=Ingenier%C3%ADa_social_%28seguridad_inform%C3%A1tica%29&oldid=10389750>.

WIKIPEDIA, La enciclopedia libre. Nessus [en línea]. [Fecha de consulta: 11 de septiembre de 2007].Disponible en <http://es.wikipedia.org/w/index.php?title=Nessus&oldid=10727188>.

WIKIPEDIA, La enciclopedia libre. Nessus (software). [en línea]. [Fecha de consulta: 12 de septiembre de 2007]. Disponible en <http://en.wikipedia.org/w/index.php?title=Nessus_%28software%29&oldid=162525325>

WIKIPEDIA, La enciclopedia libre. Netfilter/Iptables. [en línea]. [Fecha de consulta: 23 de octubre de 2007]. Disponible en: <http://es.wikipedia.org/wiki/Netfilter/iptables#iptables>

WIKIPEDIA, La enciclopedia libre. Nmap [en línea]. [Fecha de consulta: 9 de septiembre de 2007]. Disponible en <http://es.wikipedia.org/w/index.php?title=Nmap&oldid=12399383>.

WIKIPEDIA, La enciclopedia libre. Operación y Seguridad de VNC [en línea]. [Fecha de consulta: 11 de septiembre de 2007]. Disponible en: <http://en.wikipedia.org/wiki/VNC>

WIKIPEDIA, La enciclopedia libre. Proxy [en línea]. [Fecha de consulta: 26 de septiembre de 2007]. Disponible en <http://es.wikipedia.org/w/index.php?title=Proxy&oldid=12055954>.

WIKIPEDIA, La enciclopedia libre. RPC [en línea]. [Fecha de consulta: 11 de septiembre del 2007]. Disponible en <http://es.wikipedia.org/w/index.php?title=RPC&oldid=10312958>.

WIKIPEDIA, La enciclopedia libre. Secure Shell [en línea]. [Fecha de consulta: 23 de 2007]. Disponible en: <http://es.wikipedia.org/wiki/Secure_Shell>

WIKIPEDIA, La enciclopedia libre. Sistema de detección de intrusos [en línea]. [Fecha de consulta: 26 de septiembre de 2007]. Disponible en <http://es.wikipedia.org/w/index.php?title=Sistema_de_detecci%C3%B3n_de_intrusos&oldid=11187021>.

WIKIPEDIA, La enciclopedia libre. Spam [en línea]. [Fecha de consulta: 25 de septiembre de 2007]. Disponible en <http://es.wikipedia.org/w/index.php?title=Spam&oldid=12305593>.

WIKIPEDIA, La enciclopedia libre. Spoofing [en línea]. [Fecha de consulta: 25 de septiembre de 2007]. Disponible en <http://es.wikipedia.org/w/index.php?title=Spoofing&oldid=11963214>.

WIKIPEDIA, La enciclopedia libre. Squid [en línea]. [Fecha de consulta: 23 de octubre de 2007]. Disponible en: <http://es.wikipedia.org/w/index.php?title=Squid&oldid=11680379>.

WIKIPEDIA, La enciclopedia libre. Tcpdump [en línea]. Agosto 12 de 2007 [Fecha de consulta: 16 de septiembre de 2007]. Disponible en: <http://es.wikipedia.org/w/index.php?title=Tcpdump&oldid=12350613>.

WIKIPEDIA, La enciclopedia libre. TCP Wrapper [en línea]. [Fecha de consulta: 27 de septiembre de 2007].Disponible en <http://es.wikipedia.org/w/index.php?title=TCP_Wrapper&oldid=12360698>.

WIKIPEDIA, La enciclopedia libre. Troyano (informática) [en línea]. [Fecha de consulta: 25 de septiembre de 2007]. Disponible en <http://es.wikipedia.org/w/index.php?title=Troyano_%28inform%C3%A1tica%29&oldid=12270830>

WIKIPEDIA, La enciclopedia libre. VNC. Virtual Network Computing [en línea]. [Fecha de consulta: 10 de septiembre de 2007]. Disponible en: http://es.wikipedia.org/wiki/VNC

WIKIPEDIA, La enciclopedia libre. Virus informático [en línea]. [Fecha de consulta: 25 de septiembre de 2007]. Disponible en <http://es.wikipedia.org/w/index.php?title=Virus_inform%C3%A1tico&oldid=12288392>

Wrappers. [en línea]. [Fecha de consulta: 23 de octubre de 2007]. Disponible en: <http://ron.proz.com/kudoz/1838932>.