Universidad Austral de Chile

Facultad de Ciencias de la Ingeniería
Escuela de Electricidad y Electrónica

SEGURIDAD EN REDES INFORMATICAS

Trabajo de Titulación para optar al
Título de Ingeniero Electrónico

JOSE MARDONES FERNÁNDEZ
Ingeniero Electrónico
Profesor Patrocinante

JUAN IGNACIO MAURICIO ISLA CORTES

VALDIVIA 2005

Comisión de Titulación

Profesor Patrocinante:	JOSE MARDONES FERNÁNDEZ Ingeniero Electrónico
Profesores Informantes :	PEDRO REY CLERICUS Ingeniero Electrónico
	LUIS AMPUERO Ingeniero Electrónico

Fecha Examen de Titulación: 19 de Enero de 2006.-

AGRADECIMIENTOS

Agradezco a mis profesores que me apoyaron para realizar este trabajo. A mi profesor patrocinante, Don José Mardones por la paciencia y apoyo que me dio durante todo el tiempo que tomo la realización de este. A Don Pedro Rey que me aconsejaba durante el periodo en que se torno difícil terminar este trabajo, y a Luis Ampuero por la buena disponibilidad que tuvo para orientarme en el desarrollo de las ideas. .

Agradezco también a Don Franklin Castro, que más que un profesor a sido un amigo y un guía, que me apoyo en los momentos más triste de mi vida durante mi vida universitaria, a los profesores del Instituto de Ingeniería Eléctrica, las secretarias, en especial a Ximena , que de alguna u otra forma contribuyeron a mi labor con su experiencia y consejos. Hago también extensivo los agradecimientos a Don Raul, que me dio el apoyo incondicional frente a los problemas académicos.

A todos los profesores, tanto de la facultad como de otras facultades que creyeron en mi cuando emprendía nuevos proyectos universitarios, a todos ustedes muchas gracias, y a mis amigos/as, incondicionales, que en las buenas, y en especial en las malas estuvieron dándome su apoyo y cariño incondicional, gracias amigos/as, gracias a la Yoya y a ti Marisol por tu hermandad.

Dedicatoria

Quisiera expresar mi agradecimiento por el apoyo incondicional de mi madre y abuelitos, que me acompañaron en este viaje, a mi tía Mari que no alcanzo a compartir este logro. A ti Martita, por el apoyo en los últimos meses y tu amor, a Fernandita y Barbarita, por su alegría y cariño.

Dedico en especial este trabajo a mi TATA por su abnegada dedicación e inmenso cariño que hoy permite ver cumplida una de mis más anheladas metas, esta tesis es para ti.

INDICE

INDICE FIGURAS

INDICE TABLAS

I. RESUMEN

Fue realizado este trabajo para entregar el conocimiento básico a usuarios de redes informáticas que no posean ningún tipo de conocimiento previo en redes informáticas, buscando un equilibrio tanto en materias técnicas referentes a la configuración física de ellas, como a la configuración lógica de las mismas.

Se planteó una entrega de conocimientos relacionados a la gestación de las redes informáticas, prosiguiendo con los protocolos de comunicación que se desarrollaron para la compatibilidad de las plataformas desarrolladas con los años.

La definición de seguridad, junto a los niveles existentes de ella toma una orientación teórica, llegando a identificar que es lo que se quiere proteger, junto a que se entiende por amenazas o ataques.

Después de analizar los métodos de espionajes, se desarrollaron los conceptos de ataques, junto a lo que es la teoría de los agujeros de seguridad. Posterior a estos conceptos, se definió lo que es el dispositivo de protección usado en todas las redes informáticas, Firewall, el cual puede ser configurado de diferentes formas y en diferentes plataformas informáticas.

Al final, se trato la forma como se planifica una política de seguridad, la cual utiliza todos los conceptos explicados a través del trabajo realizado.

I. SUMMARY

This report was carried out in order to give basic information to the users of informatic networks who have no previous knowledge about this topic, searching for an equilibrium in technical matters referred to their physical configuration, as well as their logic configuration.

A handing over of knowledge related to informatic networks development was planned, following with the communication protocol developed for the compatibility of the platforms which evolved within time.

Security's definition, together with its existing levels of it takes a theoretical direction, identifying what is to be protected, together with the meaning of threats or attacks.

After analyzing hacking methods, the concept of attacks was developed, together with security holes theory. After these concepts, the protection dispositive used in every informatic network, firewall, was defined, which can be configurated in several ways and in different informatic platforms.

Finally we dealt with the manner in which a security policy is planned, which makes use of all the concepts explained through the executed report.

It is concluded that the responsability of the users in informatic networks is crucial, since the ignorance of their use and of the security policies of the organizations in which their are found, create the vulnerabilities to informatic attacks.

II. INTRODUCCIÓN

Al reducirse los costos de adquisición de computadores, y al disminuir el precio de conexión a un ISP, las redes informáticas han aumentado y por ende, han aumentado los usuarios de Internet en el hogar, los cuales representan un octavo de la población mundial, siguiendo en aumento, de acuerdo a las estadísticas publicadas por Nielsen/NetRatings, www.nielsennetratings.com. Las estadísticas de la consultora revelan que 498 millones de personas en el mundo tienen acceso a Internet, de las cuales 24 millones la usaron por primera vez durante el último trimestre de 2001 y 15 millones en el tercer trimestre. Adicionalmente, Nielsen estimó que un 40% de los usuarios están localizados en Estados Unidos y Canadá, mientras que un 27% en el Medio Oriente y en África. La región del Asia Pacífico cuenta con 110.1 millones de accesos residenciales a *Internet*, mientras que en Latinoamérica la cifra llega a 20.4 millones y en el resto del mundo es de 41 millones, lo que equivale a un 8% del total. El estudio se llevó a cabo entre Octubre y Diciembre del año 2001.

La agencia de noticias Reuters, reportó que las suscripciones a servicios ADSL en Japón pasó la marca de los dos millones, de acuerdo a una nueva investigación del Multimedia Research Institute, que indicó que el número de usuarios ADSL alcanzó los 2.08 millones en Febrero del 2002, ascendiendo de los 1.52 millones registrados hacia fines del 2001. Asimismo, el número de conexiones a través del cable aumentó de 1.3 millones en Diciembre del 2001 a 1.39 millones a fines de Febrero del 2002, mientras que el liderazgo entre los proveedores del servicio lo mantienen Nippon Telegraph y Telephone Corporation con un 40% del mercado, seguidos por Yahoo BB con un 21,9%. Cable Modem ha sido quien reporta el dominio del mercado de banda ancha.

El desarrollo de las redes informáticas, han propiciado la incorporación de nuevos “genios programadores”, los cuales han diseñado sistemas operativos como Linux, que permite un manejo personalizado, tanto de los sistemas informáticos como de las redes de comunicaciones en los que operan. Con esto se fue dividiendo los tipos de usuarios, y no se refiere a avanzados o básicos, sino que a usuarios que emplean las redes para con fines normales, mientras que otros para fines maliciosos. Estos últimos conocidos como Crackers y Hackers, son los que componen la fuerza de usuarios, que sólo desean apoderarse de información, destruirla o modificarla, todo

ello , para conseguir los objetivos personales que ellos persiguen. Ellos aprovechan los errores en los códigos de programación de los sistemas operativos. Por ello es muy importante que la información sea protegida. Para esto se han desarrollado sistemas basados en hardware como en software. Estos son los conocidos Firewall, screen routers, proxy, entre otros. Los avances técnicos en estos sistemas, van siendo violados, generando así una necesidad de generar nuevos sistemas de seguridad. Por todo esto, es de suma importancia poder conocer y entender los términos, como también, la forma de cómo protegerse de estos usuarios que atacan las computadoras. Es la intención este trabajo de tesis, poder encontrar las preguntas y responderlas, y poder conocer lo que sucede en esta área de las redes informáticas, la SEGURIDAD INFORMATICA.

La seguridad informática, no solo se entiende en función de ataques de Crackers o Hackers, virus o intrusos, sino en la seguridad de mantener la información intacta, esto quiere decir, además de nos ser robada o copiada la información, esta no se debe perder o alterar por personas que no sean administradores o usuarios validos de algún sistema informático. Es por ello que la seguridad pasa a ser, además, un componente físico, esto quiere decir que es importante que los sistemas tengan un resguardo físico, esto es, que se mantengan salas reservadas para servidores y back up de los sistemas de almacenamiento de datos. Por ello es muy importante conocer que se entiende por seguridad física, además de la seguridad lógica de los sistemas informáticos.

La metodología seguida fue la investigación bibliográfica, revisando libros del tema, e-book relacionados al tema, además artículos de encontrados en Internet..

La importancia de este trabajo se radico en la necesidad de generar un conocimiento claro y ordenado, que le permita a quien lo estudie, un conocimiento básico, suficiente para estudiar y desarrollar los conceptos relacionados a seguridad informática, permitiendo generar políticas de seguridad propias, resguardando la información almacenada en los sistemas utilizados

CAPITULO I
TCP/IP Y MODELO OSI

1.1 Historia de TCP/IP[1][2]

TCP/IP es una colección de protocolos estándar de la industria, diseñada para intercomunicar grandes redes (WANs = Wide Area Networks). Las siglas TCP/IP provienen de Transmission Control Protocol / Internet Protocol. Se creó en los años 60, cuando en los Estados Unidos, se estaba desarrollando una forma de comunicación entre los puntos vitales de este país, en caso de una guerra nuclear. Esta red era la que mantenía el control de la defensa de los E.E.U.U, por lo que no debía ser fundada en un sistema lineal. Esto quiere decir, que no debía perderse la comunicación entre un punto emisor y otro receptor, en el caso de que se cortara un lazo de comunicación. No debía existir, ninguna "autoridad central", ya que sería el primer blanco de ataque, por lo tanto, esta red se descentralizó, así, toda máquina conectada a esta red tenía el mismo status y capacidad para controlar y recibir información. Entonces, se decidió que los mensajes deberían dividirse en pequeñas porciones de información o **paquetes,** los cuales contendrían la dirección de destino, pero sin especificar una ruta para su arribo; por el contrario, cada paquete buscaría la manera de llegar al destinatario por las rutas disponibles y el destinatario reensamblaría los paquetes individuales para reconstruir el mensaje original. La ruta que siguen los paquetes no es de importancia, lo importante es la llegada a su destino.

En 1968, Inglaterra experimentaba con los mismo conceptos en le laboratorio Nacional de Física de la Gran Bretaña, estableciéndose la primera red experimental británica. Por este motivo, el Pentágono de E.E.U.U. comenzó a financiar un proyecto a través del Defense Advanced Research Projects Agency, DARPA. Así, en1969 DARPA establece la primera red universitaria en la Universidad de California (UCLA), surgiendo, tiempo después, nuevas redes adicionales, estableciéndose ARPANET (Advanced Research Projects Agency Network).

En resultado de la aparición de esta nueva red, se fijaron protocolos afines que permitieran la comunicación entre sistemas informáticos que contaban con diferentes tecnologías tanto de sistemas, como de comunicación. Por otra parte, se crearon diferentes alternativas de enlaces (links) de comunicaciones, pudiendo referirse a sistemas satelitales y de radio. Así, comenzó a

tomar forma las nuevas tecnologías de redes, dando como resultado el TCP/IP. Sin embargo, para aumentar la aceptación y uso de este protocolo, DARPA suministró una implementación de bajo costo a los usuarios de esta nueva comunidad de información, siendo esta implementación dirigida al sistema BSD Unix de Universidad de California.

DARPA, fundó una compañía llamada, Bolt Beranek and Newman Inc. [2], que desarrolló la implementación de TCP/IP en BSD Unix. Este desarrollo ocurre al mismo tiempo que en muchos lugares se encontraban en proceso adopción y desarrollo de tecnología de redes de áreas locales. Para Enero de 1983, se encontraban en red todos los computadores de ARPANET, utilizando los nuevos protocolos de TCP/IP.

ARPANET, era utilizada por un selecto grupo de departamentos y agencias gubernamentales, por ello, la Fundación Nacional para la Ciencia (National Science Foundation) creo la NSFNet, la cual usó exitosamente los mismos protocolos que ARPANET. Estos consistieron en una red backbone (columna vertebral) que conectó todos los centros de súper computadoras en E.E.U.U, y una serie de redes más pequeñas. La red NSFNet, unió a seis centros de súper de computadoras, en un principio, en San Diego, Boulder, Camping, Pittsburg, Ithaca y Princeton, figura 1.1.

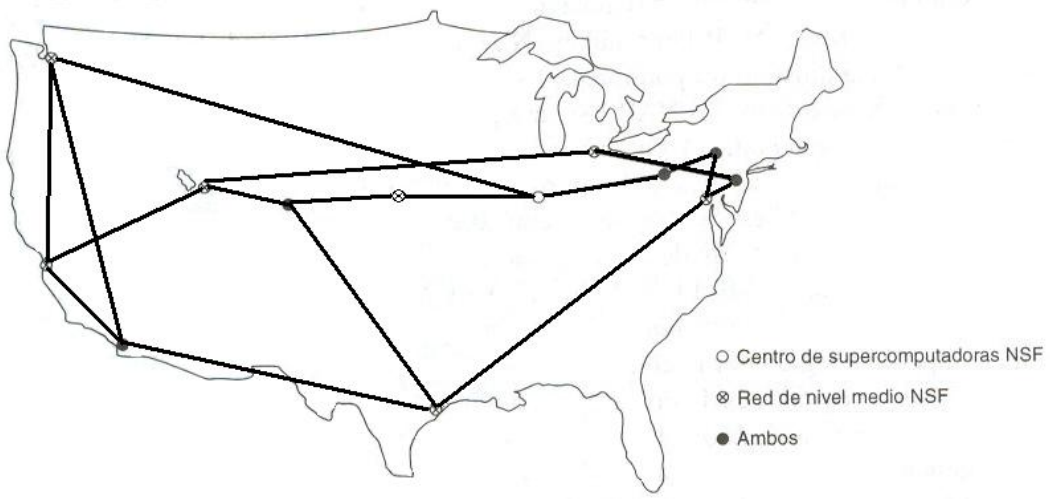


Figura 1.1 Mapa de referencia U.S.A

A estas súper computadoras, se le conectaron pequeñas computadoras LSI-11, las cuales fueron conocidas como FUZZBALL, las cuales fueron conectadas a líneas conmutadas rentadas de 56 Kbps, y formaron una subred [2], utilizando la misma tecnología que uso ARPANET. Así se convirtieron en la primera WAN de TCP/IP.

Posteriormente, la National Science Foundation financió cerca de 20 redes regionales, las que conectadas a este backbone, de NSFNet, permitieron a usuarios de miles de universidades, laboratorios de investigación, bibliotecas y museos acceder a cualquiera de las súper computadoras y comunicarse entre sí. NSFNet, fue conectada a ARPANET, en la sala de computadoras de la universidad de Carnegie – Mellon, en E.E.U.U.

Las redes conectadas a NSFNet, comprenden redes y ordenadores conectados a clases muy diferentes, con hardware y software incompatibles en muchos casos, además de todos los medios y formas posibles de conexión. Es aquí donde se encuentra una de las grandes ventajas del TCP/IP, pues este protocolo se encarga de que la comunicación entre todos sea posible. **TCP/IP es compatible con cualquier sistema operativo y con cualquier tipo de hardware**.

Desde ese momento, el uso de TCP/IP se ha incrementado en una tasa fenomenal, como también número de conexiones de Internet y las redes globales.

TCP/IP no es un simple protocolo, sino que consiste en una serie de protocolos , cada uno proveyendo un servicio específico, como http, ftp, e-mail, telnet, etc.

Debido al instantáneo éxito y sobre carga de esta red, la National Science Foundation comenzó a planear la sucesión de esta red, concediendo un contrato a MERIT, del estado de Michigan en E.E.U.U., para que la operaran. De esta forma se rentaron, a MCI, canales de fibra óptica de 448 Kbps, usando routers IBM RS6000. Al poco tiempo este nuevo backbone, de la red NSFNet, fue superada, y para 1990 subió a un segundo nivel, a 1.5 Mbps (Tecnología ATM). Al correr el tiempo, la National Science Foundation, se dió cuenta que no podía seguir financiando el uso de las redes, por ello la NSF, animó a MERIT, MCI e IBM a formar una corporación no lucrativa, ANS (Advanced Network and Services); así se inició el primer paso a la

comercialización de Internet. En ese mismo año, ANS y NSFNet subieron los enlaces desde 1.5 Mbps a 45 Mbps, formando ANSNet. En 1991, el congreso norteamericano aprobó un documento que autorizó a NREN, la Red Nacional Educativa y de Investigación, como la sucesora de NSFNet. Con el tiempo aumento su velocidad de operación a él orden de los gigabits. En 1989, México tuvo la primera conexión a Internet a través del Instituto Tecnológico de Estudios Superiores de Monterrey, el cual utilizó una línea privada analógica de 4 hilos para conectarse a la Universidad de Texas a una velocidad de 9600 bits por segundo.

1.2 Descripción modelo OSI [1][2]

Las redes de comunicaciones, están basadas en capas las cuales permiten la comunicación de los datos en una red. Para comprender la forma en que los protocolos trabajan, se han creado modelos de referencias. Los modelos más importantes son el modelo OSI y TCP.

El modelo OSI, se basa en la propuesta que desarrollo de la Organización Internacional de Normas (ISO, en inglés), siendo la primera estandarización internacional de los protocolos (norma ISO- 7494) que se usan en las diversas capas [1]. Se llama a este, modelo de referencia OSI, siendo su significado Open Systems Interconection, **interconexión de sistemas abiertos**. No es un estándar de comunicaciones, sino un lineamiento funcional para las tareas de comunicaciones, sin embargo, muchos estándares y protocolos cumplen con los lineamientos del modelo. El modelo, nace como una necesidad de informar los elementos que participan en la solución de los problemas de comunicación entre equipos de diferentes fabricantes[9].

El modelo OSI consta de siete capas numeradas, donde cada una de ellas cumple una función específica. Las siete capas del modelo OSI se ilustran en la figura 1.2.

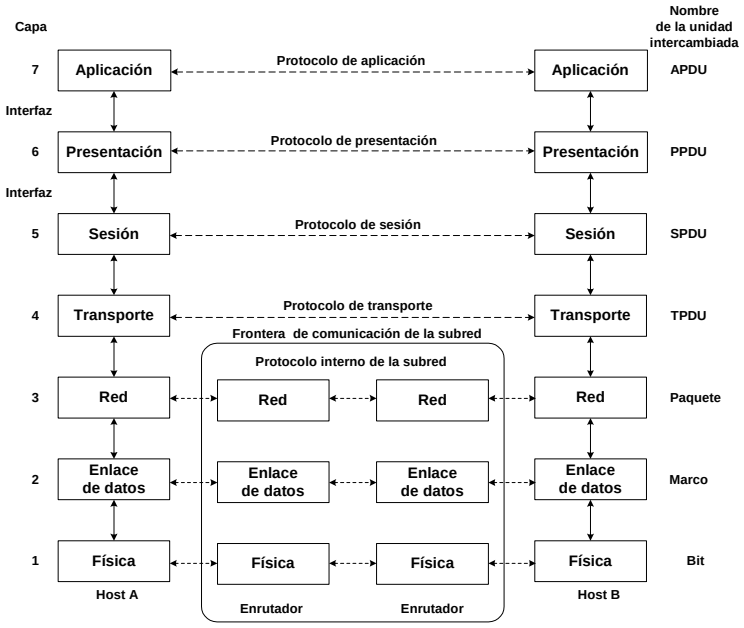


Figura 1.2. Modelo OSI

Capa 1: La capa física

La misión principal de esta capa es transmitir bits por un canal de comunicación, de manera que cuanto lo envíe el emisor, estos lleguen sin alteración al receptor.

La capa física proporciona sus servicios a la capa de enlace de datos, definiendo las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales, relacionando la agrupación de circuitos físicos a través de los cuales los bits son transmitidos.

Sus principales funciones las podemos resumir en:

- Definir las características materiales (componentes y conectores mecánicos) y eléctricas (niveles de tensión) que se van a usar en la transmisión de los datos por los medios físicos.
- Definir las características funcionales de la interfaz (establecimiento, mantenimiento y liberación del enlace físico).
- Transmitir el flujo de bits a través del medio.
- Manejar voltajes y pulsos eléctricos.

- Especificar cables, conectores y componentes de interfaz con el medio de transmisión, polos en un enchufe, etc.
- Garantizar la conexión (aunque no la fiabilidad de ésta).

Esta capa solamente reconoce bits individuales.

En esta capa, los medios de transmisión que se encuentran son:

- Físico

  Par trenzado (twisted pair).

  Cable coaxial.

  Fibra óptica.
- Inalámbrico

  Radio.

  Microondas.

  Infrarrojo..

  Ondas de luz.

Capa 2: La capa de enlace de datos

La capa de enlace proporciona sus servicios a la capa de red, suministrando un tránsito de datos confiable a través de un enlace físico.

Se ocupa del direccionamiento físico; la topología de red, el acceso a la misma, la notificación de errores, la formación y entrega ordenada de datos y control de flujo.

Su principal misión es convertir el medio de transmisión en un medio libre de errores de cualquier tipo, realizando para ello las siguientes funciones:

- Establecer los medios necesarios para una comunicación confiable y eficiente entre dos máquinas en red.
- Agregar una secuencia especial de bits al principio y al final de los paquetes de datos, estructurando este flujo bajo un formato predefinido, denominado **trama** , que suele ser de unos cientos de bytes.
- Sincronizar el envío de las tramas, transfiriéndolas de una forma confiable libre de errores. Para detectar y controlar los errores se añaden bits de paridad, se usan **CRC** (Códigos Cíclicos Redundantes) y envío de acuses de recibo positivos y negativos, y para evitar tramas repetidas se usan números de secuencia en ellas.

- Controlar la congestión de la red.
- Regular la velocidad de tráfico de datos.
- Controlar el flujo de tramas mediante protocolos que prohíben que el remitente envíe tramas sin la autorización explícita del receptor, sincronizando así su emisión y recepción.
- Encargarse del acceso de los datos al medio (soportes físicos de la red).

Capa 3: La capa de red

La capa de red proporciona sus servicios a la capa de transporte, siendo una capa compleja que proporciona conectividad y selección de la mejor ruta para la comunicación entre máquinas que pueden estar ubicadas en redes geográficamente distintas.

Es la responsable de las funciones de conmutación y enrutamiento de la información (direccionamiento lógico), proporcionando los procedimientos necesarios para el intercambio de datos entre el origen y el destino, por lo que es necesario que conozca la topología de la red (forma en que están interconectados los nodos), con objeto de determinar la ruta más adecuada.

Las principales funciones son:

- Dividir los mensajes de la capa de transporte (segmentos) en unidades más complejas, denominadas **paquetes**, a los que asigna las direcciones lógicas de los host que se están comunicando.
- Conocer la topología de la red y manejar el caso en que la máquina origen y la máquina destino estén en redes distintas.
- Encaminar la información a través de la red en base a las direcciones del paquete, determinando los métodos de conmutación y enrutamiento a través de dispositivos intermedios (routers).
- Enviar los paquetes de nodo a nodo usando un circuito virtual o data gramas.
- Ensamblar los paquetes en el host destino.

En esta capa es donde trabajan los routers, dispositivos encargados de encaminar o dirigir los paquetes de datos desde el host origen hasta el host destino a través de la mejor ruta posible entre ellos.

Capa 4: La capa de transporte

La capa de transporte proporciona sus servicios a la capa de sesión, efectuando la transferencia de datos entre dos entidades de sesión. Para ello, divide los datos originados en el host emisor en unidades apropiadas, denominadas **segmentos**, que vuelve a reensamblar en el sistema del host receptor.

Mientras que las capas de aplicación, presentación y sesión están relacionadas con aspectos de las aplicaciones de usuario, las tres capas inferiores se encargan del transporte de datos. Además, la capa de transporte es la primera que se comunica directamente con su capa de destino, ya que la comunicación de las capas anteriores es de tipo máquina a máquina.

La capa de transporte intenta suministrar un servicio de transporte de datos que aísle las capas superiores de los detalles del mismo, encargándose de conseguir una transferencia de datos segura y económica y un transporte confiable de datos entre los nodos de la red. Para ello, la capa de transporte establece, mantiene y determina adecuadamente los circuitos virtuales, proporcionando un servicio confiable mediante el uso de sistemas de detección y recuperación de errores de transporte.

Se conocen con el nombre de **circuitos virtuales** a las conexiones que se establecen dentro de una red. En ellos no hay la necesidad de tener que elegir una ruta nueva para cada paquete, ya que cuando se inicia la conexión se determina una ruta de la fuente al destino, ruta que es usada para todo el tráfico de datos posterior.

Se resumen las funciones de la capa de transporte en los siguientes puntos:

- Controlar la interacción entre procesos usuarios en las máquinas que se comunican.
- Incluir controles de integración entre usuarios de la red para prevenir perdidas o doble procesamiento de transmisiones.
- Controlar el flujo de transacciones y el direccionamiento de procesos de maquina a procesos de usuario.
- Asegurar que se reciban todos los datos y en el orden adecuado, realizando un control de extremo a extremo.
- Aceptar los datos del nivel de sesión, fragmentándolos en unidades más pequeñas aptas para el transporte confiable, llamadas segmentos, que pasa luego a la capa de red para su envío.

- Realizar funciones de control y numeración de las unidades de información (segmentos).
- Reensamblar los mensajes en el host destino, a partir de los segmentos que lo forman.
- Garantizar la transferencia de información a través de la red.

Capa 5: La capa de sesión

La capa de sesión proporciona sus servicios a la capa de presentación, proporcionando el medio necesario para que las entidades de presentación de dos host, que se están comunicando por red, organicen y sincronicen su diálogo y procedan al intercambio de datos. Sus principales funciones son:

- Establecer, administrar y finalizar las sesiones entre dos hosts que se están comunicando.
- Si por algún motivo una sesión falla por cualquier causa ajena al usuario, restaurar la sesión a partir de un punto seguro y sin perdida de datos o, si esto no es posible, terminar la sesión de una manera ordenada, chequeando y recuperando todas sus funciones, evitando así problemas en sistemas transaccionales.
- Sincronizar el diálogo entre las capas de presentación de los dos hosts y administrar su intercambio de datos, estableciendo las reglas o protocolos para el diálogo entre máquinas, regulando quien habla y por cuanto tiempo.
- Conseguir una transferencia de datos eficiente y un registro de excepciones acerca de los problemas de la capa de sesión, presentación y aplicación.
- Manejar **tokens** . Los tokens son objetos abstractos y únicos que se usan para controlar las acciones de los participantes en la comunicación, base de ciertos tipos de redes, como Token Ring o FDDI.
- Hacer **check** |**points**, que son puntos de recuerdo en la transferencia de datos, necesarios para la correcta recuperación de sesiones perdidas.

Capa 6: La capa de presentación

La capa de presentación proporciona sus servicios a la capa de aplicación, garantizando que la información que envía la capa de aplicación de un sistema pueda ser entendida y utilizada por la capa de aplicación de otro, estableciendo el contexto sintáctico del diálogo.

Su tarea principal es aislar a las capas inferiores del formato de los datos de las aplicaciones específicas, transformando los formatos particulares (ASCII, EBCDIC, etc.) en un formato común de red, entendible por todos los sistemas y apto para ser enviado por red. Es también las responsable de la obtención y de la liberalización de la conexión de sesión cuando existan varias alternativas disponibles.

Para cumplir estas funciones, la capa de presentación realiza las siguientes operaciones:

- Traducir entre varios formatos de datos utilizando un formato común, estableciendo la sintaxis y la semántica de la información transmitida. Para ello convierte los datos desde el formato local al estándar de red y viceversa.
- Definir la estructura de los datos a transmitir. Por ejemplo, en el caso de un acceso a base de datos, definir el orden de transmisión y la estructura de los registros.
- Definir el código a usar para representar una cadena de caracteres (ASCII, EBCDIC, etc).
- Dar formato a la información para visualizarla o imprimirla y comprimir los datos si es necesario.
- Aplicar a los datos procesos criptográficos cuando sea necesario.

Capa 7: La capa de aplicación

La capa de aplicación es la capa del modelo OSI más cercana al usuario, y está relacionada con las funciones de más alto nivel, proporcionando soporte a las aplicaciones o actividades del sistema, suministrando servicios de red a las aplicaciones del usuario y definiendo los protocolos usados por las aplicaciones individuales.

Es el medio por el cual los procesos, las aplicaciones de usuario, acceden a la comunicación por red mediante el entorno OSI, proporcionando los procedimientos precisos para ello.

Los procesos de las aplicaciones se comunican entre sí por medio de entidades de aplicación propias, estando éstas controladas por protocolos específicos de la capa de aplicación, que a

su vez utilizan los servicios de la capa de presentación, situada inmediatamente debajo en el modelo.

Difiere de las demás capas debido a que no proporciona servicios a ninguna otra capa OSI, sino solamente a aplicaciones que se encuentran fuera del modelo (procesadores de texto, hojas de cálculo, navegadores web, etc.).

La capa de aplicación establece la disponibilidad de los diversos elementos que deben participar en la comunicación, sincroniza las aplicaciones que cooperan entre sí y establece acuerdos sobre los procedimientos de recuperación de errores y control de la integridad de los datos.

La estructura del modelo OSI consta de 5 partes:

A. **Estructura multi-nivel**: diseñada con la idea de que cada nivel pueda resolver solamente una parte del problema de la comunicación, con solo funciones específicas.

B. **Un nivel superior utiliza los servicios de los niveles inferiores**: esto debido a que cada nivel se comunica con un nivel homologo en otras máquinas. La comunicación entre niveles es definida de manera que el nivel N utilice los servicios del nivel N-1, y a su vez , el nivel N, proporcione servicios al nivel N+1.

C. **Puntos de accesos**: lo que se refiere a interfaces entre los niveles para los servicios de los niveles.

D. **Dependencia de niveles**: esto ya que por lo tratado en el punto B, los niveles dependen del nivel anterior , como del posterior.

E. **Encabezados:** se incorporan en cada nivel uno, al mensaje, en un formato de control, el cual permite que el receptor se entere que un emisor está enviando un mensaje con información.

En cualquier nivel se introduce un encabezado al mensaje, por ello se considera que un mensaje está constituido por dos partes, el encabezado y la información (datos). Esta incorporación de encabezados es necesaria , aunque significa que aumenta el tamaño del mensaje, esto implica un mensaje voluminoso. Como en el receptor, se invierte el proceso señalado , el mensaje original, la información (dato), llega intacto, figura 1.3.

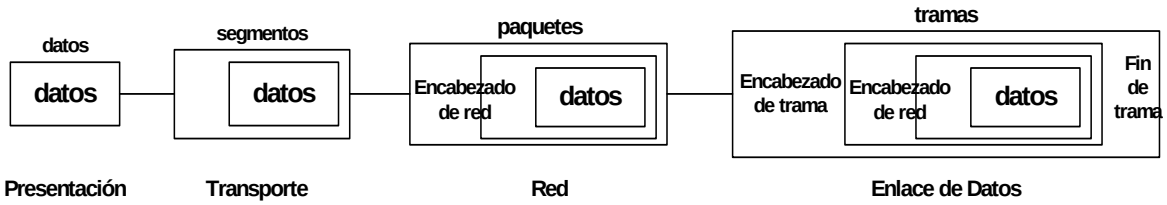


Figura1.3. Encapsulado

1.3 Modelo TCP/IP

La mayoría de las redes se dividen por niveles o capas para tener una mejor organización, al momento de recibir o enviar datos. Esto es, porque cada capa tiene una función para brindar un servicio en la transmisión o recepción de datos, que la capa superior o inferior no la conoce.

El modelo TCP/IP tuvo origen en el modelo de redes OSI de las siete capas, agrupando algunas de estas, quedando cuatro en total, como se ilustra en la figura 1.4.

Fue creado cuando se añadieron redes de satélites y radio, debido a que los protocolos existentes tuvieron problemas para interactuar con ellas, de modo que se necesitó una nueva arquitectura, surgiendo así el modelo TCP/IP, siendo el objetivo principal la capacidad de interconectar entre si múltiples redes. Otro objetivo principal fue que la red fuese capas de sobrevivir a la pérdida del hardware de la subred, sin que las conexiones existentes se interrumpieran, permaneciendo intactas las conexiones, mientras que las máquinas de origen y destino estuvieran funcionando.

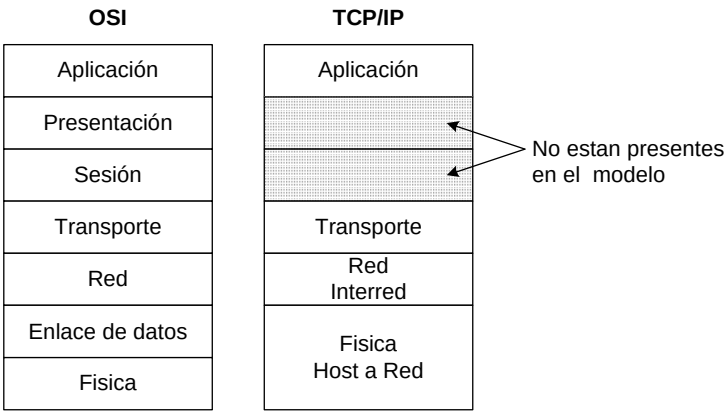


Figura 1.4. Comparación Modelos OSI y TCP/IP

Este modelo se divide en cuatros capas, las que son:

Capa Física:

Bajo la capa de red o interred, existe un gran vació. Realmente, este modelo no dice mucho sobre que se necesita en esta capa, excepto que el Host que esté conectado a la Red, use algún protocolo que permita enviar paquetes a IP (direcciones validad de internet). Se abstrae de la topología de red, puesto que la Capa de Red corre en cualquier tipo de red.

Capa de Red o Interred:

Es el eje que mantiene unida toda la arquitectura. Permite que los nodos inyecten paquetes en cualquier red y los hagan viajar de forma independiente a su destino, lo cual puede generar que los paquetes lleguen en diferente orden , lo que es solucionado por una capa superior, que reordena los paquetes recibidos. Además define un formato de paquete y protocolo oficial llamado IP , siendo también su trabajo entregar estos paquetes IP a donde deben ir. Una consideración importante es el ruteo de los paquetes, pues evita la congestión. Por ultimo, se puede concluir que es parecida a la capa de red del modelo OSI.

Los servicios de esta capa se han diseñado con los siguientes objetivos:

1. Los servicios deberán ser independientes de la tecnología de subred.
2. La Capa de Transporte debe tener oculto el número, tipo y topología de la subred, que se encuentran presentes.
3. Las direcciones de la red, que se ponen a disposición de la capa de Transporte deberán utilizar un plan de numeración uniforme, aún a través de las redes tipo LAN y WAN.

Capa de Transporte:

Se encuentra sobre la capa de red en el modelo TCP/IP. Su principal función es enriquecer la calidad de servicio de la Capa de Red. Es la más importante, su tarea es hacer que el transporte de datos se realice en forma económica y segura, entre el destino y el origen, no dependiendo esto de la cantidad de redes físicas que se encuentren en uso. Para lograr esto la capa de transporte utiliza todos los servicios que brinda la Capa de Red.

Existen dos protocolos end to end que pueden ser definidos aquí, TCP y UDP. El protocolo TCP , es confiable y orientado a la conexión, permitiendo que se entreguen los paquetes de

información de un emisor a un receptor sin errores. Estos paquetes se reordenan en la capa de interred, o red, como ya se ha mencionado antes. Además permite el control del flujo de los paquetes enviados por un emisor rápido, en comparación a un receptor más lento, permitiendo que este ultimo pueda manejar los paquetes que llegan. El protocolo UDP (user datagram protocol), no tiene conexión, no es confiable para aplicaciones que no necesiten asignación de secuencia ni control de flujo TCP.

Capa de Aplicación:

Sobre la capa de transporte se encuentra esta capa, aquí se encuentran todos los protocolos de alto nivel. Contiene los protocolos de los usuarios (aplicaciones). Los protocolos más comunes son: transferencia de archivos (FTP), acceso de archivos remotos (TELNET) , correo electrónico (SMTP), o cuando dos personas trabajan sobre computadoras distintas, para un mismo proyecto. El protocolo TELNET, permite que un usuario pueda entrar a una máquina distante y trabaje allí, FTP sirve para la transferencia de archivos de un archivo de un equipo a otro de manera más eficiente, el SMTP permite el envió de archivos. Con el tiempo se han creado nuevos protocolos como el DNS (domain name service). La figura 1.5, muestra la relación entre IP, TCP y UDP, además los protocolos nombrados.

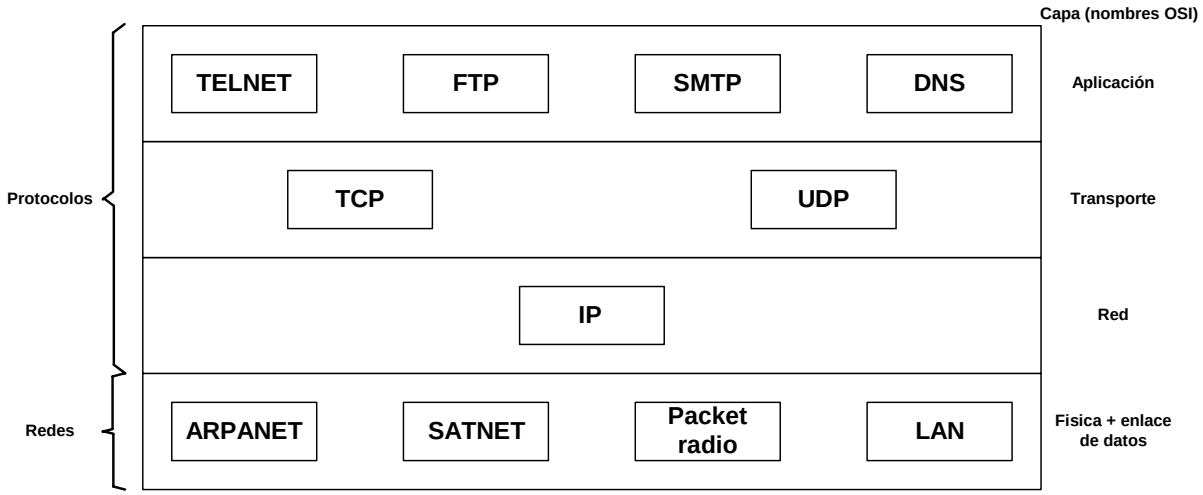


Fig. 1.5. Relación de Protocolos

1.4 Protocolos de Red y Aplicaciones [1][7]

1.4.1 Protocolos de Red

Los protocolos de red son aquellos protocolos que se emplean (o facilitan) el proceso de transporte transparentemente. Ellos son invisibles para el usuario, a menos que el usuario los emplee para monitorear los procesos de sistemas.

Los protocolos mas importantes que se pueden mencionar son:

- Protocolo de resolución de direcciones (ARP)
- Protocolo de control de comunicación de Internet (ICMP)
- Protocolo de Internet (IP)
- Protocolo de control de transmisión (TCP)
- Protocolo de usuario de datagrama (UDP)

1.4.1.1 Protocolo de resolución de direcciones (ARP)

ARP es responsable de encontrar un mapa de cualquier dirección física local de un IP que se pueda demandar. Si ARP no tiene un mapa en memoria, debe de encontrar alguno en la red. ARP usa la comunicación local (broadcast) , preguntándole a todos los sistemas en la red si tienen el IP resuelto. Esto es vital en la información de ruteo a través de la Internet. Antes que el mensaje, o cualquier dato, sea enviado, es encapsulado en paquetes IP, o bloques de información en un formato apropiado para su transporte en Internet. Este contiene el número de dirección de Internet (IP) de los equipos de origen y destinación. Antes que un paquete se envíe desde el equipo de origen, tiene que ser conocida (descubierta) la dirección del hardware receptor. Una petición ARP es enviada por la subred. Esta petición es capturada por la maquina de origen y el proceso de transferencia puede comenzar.

El diseño de ARP, incorpora un cache, que es una memoria que almacena las ultimas relaciones entre los números de direcciones de Internet (IP) con los números de hardware de las tarjetas de red (MAC), de esta manera, las direcciones de hardware de la máquinas remotas o redes son recordadas. Esto ahorra tiempo y recursos de red.

Por un lado, el llegar a conocer estas tablas, es un riesgo de seguridad, debido a que un hacker puede hacer uso de éstas para ingresar a alguna red, por algún método de re-empaquetamiento de

los paquetes de red. De esta forma se podría ingresar a algún sistema que mantiene restricciones de ingreso a través de la identificación IP. Este tipo de ataque es conocido como spoofing.

1.4.1.2 Protocolo de control de comunicación de Internet (ICMP)

Es otro protocolo de bajo nivel, raramente usado por el programador de aplicaciones. Usa datagramas IP para enviar mensajes que desempeñan un control de flujo, reportes de error, manipulación de ruteo, y otras funciones de información para TCP/IP.

Los programadores de aplicaciones, ciertamente harán uso de la utilidad ping, el cual es uno de los programas mas usados por ICMP. Ping usa la función echo del ICMP para probar la respuesta de un servidor en una red. Obteniéndose respuesta de un ping, se asegura que existe comunicación con la máquina remota.

1.4.1.3 Protocolo de Internet (IP)

Es un protocolo sin relación a nada, eso significa que no necesita una asociación end-to-end establecida antes que se transmita datos. Esto contrasta con un protocolo orientado a conexión, que intercambia información de control entre los servidores, para establecer la conexión antes de que se transmita datos. IP no garantiza la confiabilidad de la entrega de datos. Paquetes de datos pueden llegar a su destino en un orden distinto, duplicándose, o que no llegue en si. IP deja a otras capas, como la protocolo de transporte TCP, la acción de controlar y entregar la información. La construcción básica del bloque IP es el datagrama, figura 1.6. Cada datagrama, o paquete de dato, tiene una dirección de procedencia y de destinación. El enrutamiento de datos es hecho a nivel del datagrama. Como el datagrama es ruteado de una red a otra, puede llegar a ser necesario el dividir los paquetes en piezas menores. Este proceso se conoce por fragmentación, y es responsabilidad de la capa IP. La fragmentación es a veces necesaria en algunas redes, debido a la diferencia de componentes de hardware que puedan hacer que los paquetes en la red sean de distintos tamaños. IP reensambla los paquetes cuando se reciben, haciendo que el equipo de destino reciba los paquetes que se enviaron.

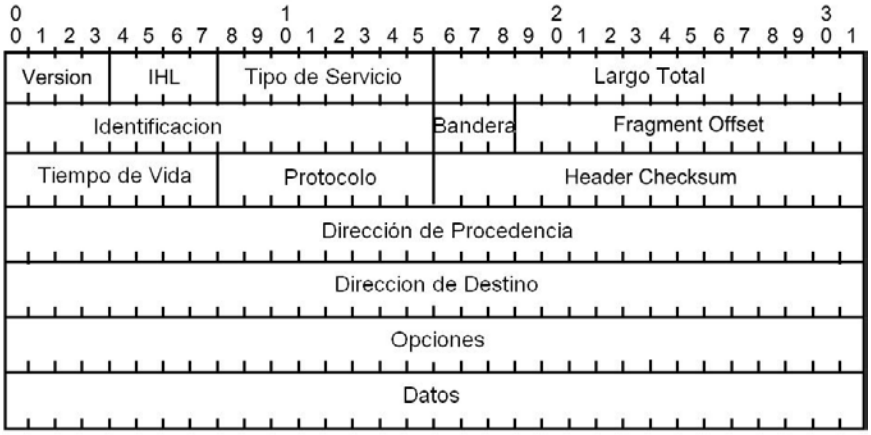


Figura 1.6. Configuración Datagrama IP

El datagrama IP, está compuesto de varias partes. La primera, es el encabezamiento o encabezado, que contiene por información general, incluyendo la dirección de origen y destino de las direcciones IP. Juntos, estos elementos forman el encabezado completo. La porción restante del datagrama contiene cualquier información, la cual es la que se conoce como dato.

1.4.1.4 Protocolo de usuario de datagrama (UDP)

Este protocolo no crea una sesión entre máquinas comunicándose antes de que los datos sean transmitidos. Por ello, UDP no garantiza que los paquetes entregados sean entregados en orden, o que serán retransmitidos si es que se pierden. Dada la inestabilidad de este protocolo, fue desarrollado por su simple cabecera, figura 1.7, que se puede comparar con la complejidad del encabezado del TCP, figura 1.8.

El datagrama UDP no tiene sincronización de parámetros o de opciones de prioridad. Todo lo que existe es el puerto de origen, puerto de destino, largo de dato, verificación de cabecera checksum y luego los datos.

Hay muchas razones por las cuales no se requiere un protocolo que establezca una sesión. Por un lado, es asociada una pequeña cabecera el UDP, donde no hay necesidad de mantener las rutas de una secuencias de números, retransmitir los tiempos, retrasos de acuse de recepción, y retransmisión de los paquetes. UDP es una rápida y perfilada funcionalidad, pero no es

garantizada. Esto hace que UDP sea perfecta para la comunicación que envuelve broadcast, anuncios generales para la red, o datos en tiempo real, porque no se ha creado una sesión entre cada equipo de recepción.

Puerto de origen	Puerto de destino
Longitud	Suma de chequeo
Dato	

Figura 1.7. Encabezado UDP

1.4.1.5 Protocolo de control de transmisión (TCP)

Verifica si el dato es entregado en orden y sin corromperse. TCP provee confiabilidad de transmisión para la conexión orientada a los flujos de bytes. La confiabilidad proviene de la inserción de la suma de chequeo en cada paquete de dato transmitido. En recepción, la suma de chequeo es generado y comparado con la suma de chequeo incluido en la cabecera de cada paquete. Si no coinciden la suma de chequeo, el receptor comunica el hecho al emisor, y el dato es retransmitido automáticamente. Un programador de aplicaciones no tiene que preocuparse de esta función porque cubre las capas inferiores. TCP es considerado orientado a conexión, porque los dos puntos finales de comunicación establecen un diálogo de negociación antes de que la transmisión se realice. Esta negociación garantiza al emisor que el receptor está presente y listo para aceptar el dato. La figura 1.8, muestra el formato del mensaje TCP. El mensaje contiene un puerto de origen y de destino de 16 bit, como lo hace el mensaje UDP. Hay que agregar que el mensaje también incluye campos de secuencia como también campos de suma de chequeo. Estas entradas adicionales en el mensaje apoya la confiabilidad del transporte de datos TCP.

Puerto de origen		Puerto de destino	
Secuencia numerica			
Numero de aceptación			
Offset	Reservado	Bandera	Ventana
Suma de chequeo		Puntero de urgencia	
Opciones		Relleno	
Dato			

Figura 1.8. Encabezado TCP

La posición de cada uno de los protocolos mencionados en las capas del modelo TCP/IP, se muestran en la figura 1.9.

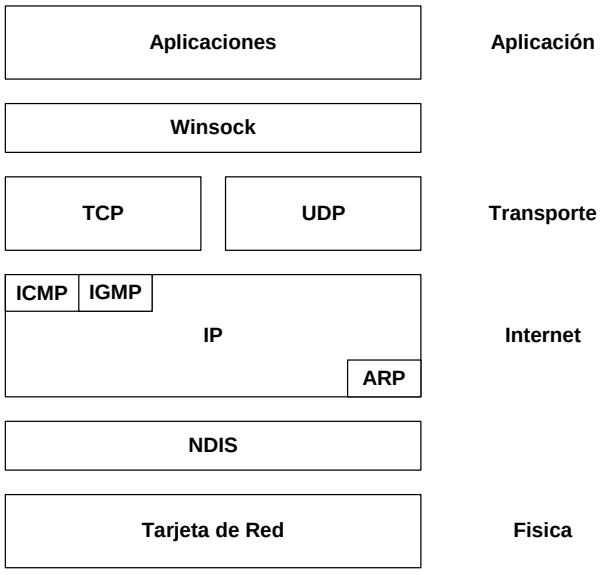


Figura. 1.9. Capas Modelo TCP/IP

1.4.2 Protocolos de aplicación

Estos protocolos trabajan en la capa más alta del modelo TCP/IP, estos protocolos además están relacionados con los puertos. Entre estos protocolos podemos encontrar los protocolos FTP, SMPT, TELNET, HTTP.

1.4.2.1 Protocolo FTP

Es un método estandarizado de transferencia de archivos desde un sistema a otro. Se propuso en la RFC 0765 como sigue:

Los objetivos de FTP son:

- Promover el intercambio de archivos
- Alentar directamente o indirectamente el uso de computadores remotos
- Proteger al usuario de la variaciones de sistemas de almacenamiento de archivos entre servidores.
- La transferencia de datos en forma segura y eficiente.

La primera definición de FTP fue en Abril de 1971, y la especificación completa se puede encontrar en RFC 114.

La transferencia de archivos FTP ocurre en condiciones cliente-servidor. La máquina que oficia de demandante ejecuta un cliente que puede estar en diferentes sistemas operativos como:

Sistema Operativo	***Cliente***
UNIX	Native, LLNLXDIR 2.0, FTPtool
Microsoft Windows 95	Native, WS_FTP, Netload, Leap FTP, Cute-FTP, SDFTP, FTP Explores
Microsoft Windows NT	Native, WS_FTP, Netload, Leap FTP, Cute-FTP, SDFTP, FTP Explores
Microsoft Windows 3.x	Win_FTP, WS_FTP, CU-FTP
Macintosh	Anarchie, Fetch, Freetp
OS/2	GibbonFTP, FTP-IT, Lynn´s Workplace FTP
VAX	Nativo

Esto genera una petición que es dirigida a un servidor de archivos, generalmente en otra red. Generalmente la petición es dirigida al puerto 21. Para que la conexión pueda ser ejecutada, debe haber un servidor FTP, corriendo en el servidor.

1.4.2.2 Protocolo SMTP

Las siglas de este protocolo significa, ***simple mail transfer protocol***. El objetivo de SMTP, es la transferencia de mensajes (mail) de forma confiable y eficiente (RFC 821). Este protocolo es sumamente liviano y eficiente. Un usuario envía una petición de SMTP a un servidor. Se estable posteriormente una conexión de dos vías (duplex connection). El cliente de mail envía una instrucción MAIL, indicando que se quiere enviar un mail a un destino en Internet. Si SMTP, permite esta operación, un reconocimiento de aceptación es enviado de vuelta a la máquina cliente. En ese momento la sección de mail comienza. Entonces , el cliente envía la identidad del destino, o la dirección IP y el mensaje es enviado. A pesar de lo simple que es SMTP, el servicio de mail es una fuente incalculable de agujeros de seguridad. La mala configuración de este servicio es la razón de los agujeros de seguridad. Los servidores SMTP son nativos del sistema UNIX generalmente, pero se han creado aplicaciones para Windows.

1.4.2.3 Protocolo TELNET

Este protocolo es descrito en el RFC 854. El propósito del protocolo TELNET es la facilidad justa de comunicación orientada a la conexión, de ocho bit, bidireccional. El objetivo principal es permitir un método de estandarizar la interfase de dispositivo terminal y al proceso de terminal orientado a cada uno. TELNET no sólo permite la conexión de un usuario a un servidor, también permite el uso de comandos en el servidor. De esa manera, una persona en un lugar remoto puede hacer un TELNET a una máquina local, y ejecutar programas, como si estuviera en el servidor local. TELNET permite ejecutar una variedad de funciones (enviar mail, por ejemplo) a un bajo costo de recursos. También permite implementar TELNET seguro (software putty) de manera fácil, y hay varios tipos de programas que permiten implementar TELNET, el mas conocido es *Secure Shell*. Para ejecutar TELNET hay que utilizar el comando, dando una dirección. Por ejemplo, sería escribir, #telnet uach.cl.

Este comando inicia una sesión TELNET, y contacta a uach.cl, y pide una conexión. Esta conexión puede ser aceptada o denegada, dependiendo de la configuración del servidor. Los clientes de TELNET operan en sistemas operativos como:

Sistema Operativo	*Cliente*
UNIX	Native
Microsoft Windows 95	Native (linea de comando), ZOC, NetTerm, Zmud, WinTel32
Microsoft Windows NT	Native (linea de comando), CRT, y los que usa Microsoft Windows 95
Microsoft Windows 3.x	Trumpet Telnet, Wintel, Ewan
Macintosh	NCSA Telnet, NiftyTelnet, Comet
VAX	Native

1.4.2.4 Protocolo HTTP

El protocolo HTTP, ***hypertext transfer protocol***, es le protocolo mas reconocido de todos por ser el que nos permite navegar por Internet. En la RFC 1945 se declara que este protocolo:

" … es un protocolo de nivel de aplicación con una distribución ágil, rápida y necesaria, colaborativa, sistema de información que combina multimedia y texto. Es genérica, desnacionalizada, protocolo orientado a objetos que puede ser usado por muchas tareas, como servidores de nombre, sistemas de administración de objetos distribuidos, a través de extensiones de los métodos de petición (comandos). Una característica de http es la clasificación de la representación de los datos, permitiendo a sistemas que se construyan independientemente de los datos que son transferidos."[2].

HTTP ha cambiado para siempre la naturaleza de Internet, primariamente por brindar Internet a las masas. Mientras que aplicaciones como TELNET, requieren que el usuario se identifique, http elimina eso. El usuario solo consume los recursos del sistema en el ínstante que pide o recibe alguna información. Usando buscadores, se pueden monitorear el proceso mientras ocurre. Para cada elemento de datos (texto, gráficos, sonido) en una página WWW, el buscador contactará el servidor una vez. De esa forma se baja primero el texto, luego los gráficos y al final los archivos de sonido, así. http, no se preocupa particularmente de que tipo de datos se requiere. Varios tipos de multimedia pueden ser incrustados en él. Los clientes para este protocolo corren en sistemas operativos como:

Sistema Operativo	*Cliente*
UNIX	Xmosaic, Netscape Navigator, Grail, Lynux, TkWWW, Arena
Microsoft Windows (todos)	Netscape Navigator, WinWeb, Mosaic, Microsoft Internet Explorer, WebSurfer, NetCruise, AOL, Prodigy
Macintosh	Netscape Navigator, MacMosaic, Mac Web, Samba, Microsoft Internet Explorer
OS/2	Web Explorer, Netscape Navigator

1.5 Puertos

En los puntos anteriores, se ha hablado de los protocolos, tanto de red como de aplicación.

En el caso de los protocolos de aplicación, también conocido como servicios. Estos están asociados a puertos, los cuales reciben una identificación numérica. Si se realiza una petición, por ejemplo de una página web, el servidor tiene que saber a quien se la envía. Esa dirección electrónica es la dirección IP, qué es un número de 4 grupos de cifras de la forma **xxx.xxx.xxx.xxx** . Pero eso no es suficiente, ya que en Internet se pueden utilizar muchos servicios diversos, y es necesario poder diferenciarlos. La forma de "diferenciarlos" es mediante números asignados a los puertos.

Imaginemos un edificio de oficinas, éste tiene una puerta de entrada al edificio (que en este caso sería la IP) y muchas oficinas que dan servicios (que en este caso serían los puertos). Eso nos lleva a que la dirección completa de una oficina viene dada por la dirección postal y el número de la oficina. En el caso de Internet viene dado por la dirección IP y por el número de puerto. Así, por ejemplo, un servidor web escucha las peticiones que le hacen por el puerto 80, un servidor FTP lo hace por el puerto 21, etc...

Entonces los puertos son los puntos de enganche para cada conexión de red que se realiza. El protocolo TCP identifica los extremos de una conexión por las direcciones IP de los dos nodos implicados (servidor y cliente), y el número de los puertos de cada nodo.

Cuando se conectan a Internet, el proveedor entrega para esa conexión, una dirección IP para poder comunicarse con el universo de Internet. Cuando se solicita un servicio de Internet,

por ejemplo una página web, se hace la solicitud de la página mediante un puerto del ordenador a un puerto del servidor web.

Existen 65.536 puertos, usados para las conexiones de Red. La tabla 1.1, muestra algunas de las relaciones que existen entre el número de puerto y el servicio que este entrega. Se debe notar, que hay puertos que son atacados por programas, conocidos como troyanos, los cuales tratan de establecer una conexión con algún puerto particular, para así tomar control de éste. Alguno de los puertos usados por troyanos se muestran en el anexo A.

Una medida básica de seguridad es conocer que puertos existen, ¿cuales están abiertos?, ¿Porque están abiertos?. De estos últimos, los que no utilicemos o que sean fuente de un problema de seguridad.

Usando el ejemplo del edificio, si se tiene una puerta de entrada, nunca se deja abierta. También existen ventanas, a las que les pones cortinas para preservar la intimidad. Pues lo mismo se aplica a un computador cuando esta conectado a Internet.

Puerto	***Descripción***
1	TCP Port Service Multiplexer (TCPMUX)
7	ECHO
18	Message Send Protocol (MSP)
20	FTP -- Data
21	FTP -- Control
22	SSH Remote Login Protocol
23	Telnet
25	Simple Mail Transfer Protocol (SMTP)
37	Time
43	WhoIs
49	Login Host Protocol (Login)
53	Domain Name System (DNS)
69	Trivial File Transfer Protocol (TFTP)
80	HTTP
109	POP2
110	POP3
137	NetBIOS Name Service
139	NetBIOS Datagram Service
143	Interim Mail Access Protocol (IMAP)
150	NetBIOS Session Service
194	Internet Relay Chat (IRC)
197	Directory Location Service (DLS)
443	HTTPS
546	DHCP Client
547	DHCP Server
563	SNEWS
569	MSN
1080	Socks

Tabla 1.1. Tabla Puertos / Descripción

Un atacante (hacker) que intente o consiga tener control sobre un computador necesita tener a su disposición una puerta abierta en el computador para poder comunicarse, es decir, un puerto de comunicaciones abierto.

Encontrando los puertos abiertos que no se utilizan deben ser cerrados, ya que es evidente que al cerrar un puerto que se esta utilizando, ese servicio deja de funcionar.
Windows como tal, no tiene demasiados puertos abiertos, por lo que es fácil comprobar si un puerto está abierto. Esto último sirve para establecer la existencia de troyanos en un computador.

Es recomendable cerrar el puerto numero 139 (netbios) de Windows, pero sólo para el protocolo TCP/IP, la opción de compartir ficheros e impresoras de Windows. Para saber que puertos existen abiertos en un computador se puede utilizar un software escaneador de Puertos. Además existen páginas web que hacen el trabajo de escanear los puertos de un computador. Una vez que se ha realizado un escaneo de puerto, hay que cerrar los puertos, esto se realizar con un software o hardware conocido como Firewalls (cortafuego).

Una ventaja añadida de los firewall es respecto a la respuesta que puede ofrecer ante un escaneo de puertos. Es decir, si un hacker escanea los puertos de un computador, este le responde que el puerto existe, pero está cerrado, el atacante, como mínimo, ya sabe que esta conectado. Lo mejor es que el computador no responda de ninguna forma, es decir, aparecer como si estuviera desconectado de Internet o indicando la inexistencia de puertos. Esa técnica de ocultación es lo que se llama modo Stealth y se realiza a través de los firewall.

CAPITULO II
TOPOLOGÍA DE REDES

Una topología de red es el patrón, modelo o estructura por el cual un medio de cableado es usado para interconectar varios computadores para así formar una red. La topología usada esta relacionada íntimamente con el protocolo de la capa de enlace de dato. La elección del tipo de cable y cableado depende del tipo de topología requerida. La cantidad de atenuación es propio al medio, la velocidad de la señal, y del largo de los segmentos de cable, y son todos factores que deben ser contados en el momento de decidir el tamaño de la red. Una topología, por consecuencia, es seleccionada, en muchos casos, como resultado de la decisión del protocolo de enlace de dato [3].

Se consideran 3 aspectos al momento de considerar una topología:

1. La topología física: es la disposición real de los host y de los cables (los medios) en la red.
2. La topología lógica: es la forma en que los hosts se comunican a través del medio. Los dos tipos más comunes de topologías lógicas son broadcast (Ethernet) y transmisión de tokens (Token Ring).

   Topología de broadcast significa que cada host envía sus datos hacia todos los demás hosts del medio de red. Las estaciones no siguen ningún orden para utilizar la red, el orden es el primero que entra, el primero que se sirve. Esta es la forma en que funciona Ethernet.

   Transmisión de tokens controla el acceso a la red al transmitir un token eléctrico de forma secuencial a cada host. Cuando un host (servidor) recibe el token, eso significa que el host puede enviar datos a través de la red. Si el host (servidor) no tiene ningún dato para enviar, transmite el token hacia el siguiente host y el proceso se vuelve a repetir.
3. La topología matemática, donde los mapas de nodos y los enlaces a menudo forman patrones.

La elección de una topología sobre otra va a tener un fuerte impacto sobre:

- El tipo de equipo que la red necesita
- Las capacidades de este equipo
- Desarrollo de la red
- La forma en que la red es manejada

Conociendo las distintas topologías, se comprenden las capacidades de los distintos tipos de redes.

Para que las computadoras puedan compartir archivos y poder transmitirlos, tienen que estar conectadas entre ellas. La mayoría de las redes usan un cable para conectar una computadora a otra, pero con el desarrollo de las tecnologías inalámbricas, se encuentran tarjetas de red inalámbricas, capaces ya de transmitir hasta 54 Mbps.

Sin embargo, esto no es tan simple como conectar un cable de una computadora a otra.

Para que una topología en red funcione bien, necesita un diseño previo. Por ejemplo, una topología en particular puede determinar el tipo de cable, y como este cableado recorre el suelo, paredes y techo.

Existen 4 tipos de topologías:

- Bus
- Anillo
- Estrella
- Malla (Mesh)

Las topologías nombradas y los diagramas topológicos de las redes representan vistas lógicas, y no necesariamente corresponden a las interconexiones físicas.

2.1 Topología Bus [3] [7][8] [10]

Los comienzos de esta configuración tiene su origen en el cable coaxial. Esta configuración permite a una red simple que un grupo de computadores puedan compartir información entre ellos. Los datos son transportados por un cable, o **bus**, a todos los computadores conectados a ella. Cuando un computador necesita comunicarse con otro, este direcciona un paquete y lo envía por el cable; para ello necesita la dirección MAC del computador que recibirá el paquete. La dirección es resuelta normalmente usando un broadcast, el que interroga a cada computador en la red por su dirección MAC. La resolución de esta dirección es manejada por TCP/IP, por el protocolo ARP.

Usando este método, los clientes y servidores pueden colocar aleatoriamente en la red datos, porque todos pueden escuchar los paquetes enviados por una máquina. Este sistema es fácil de implementar, además de ser confiable, y puede usar equipos no muy costosos, como repetidores y puentes (bridges). Sin embargo, si se le añaden más equipos a este tipo de red, se añade más tráfico, el cual compite por su transmisión, creando un embotellamiento en el tráfico de datos.

Esta topología se representa gráficamente en la figura 2.1, de la cual se observa que es un sistema serial. Si el cable se corta, el segmento completo pierde conectividad, por lo que se pierde funcionalidad hasta que se repara.

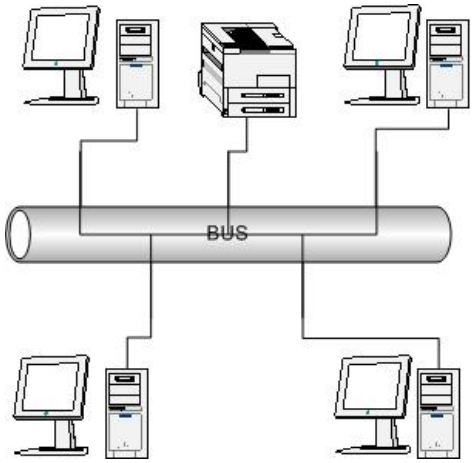


Fig. 2.1. Topología BUS

Ethernet es un ejemplo de una red de BUS común. Esta topología, puede ser cableada usando diferentes tipos de cables, como el coaxial, el cual fue el pionero. Tres son las especificaciones más populares para topologías Ethernet:

- 10BASE2, que usa un cable coaxial fino, que permite un transporte de la señal hasta 185 metros.
- 10BASE5, que usa un coaxial mas grueso, permitiendo esto una transmisión de hasta 500 metros.
- 10BASET, que usa un cable de par trenzado, que puede transportar una señal hasta 100 metros.

La topología BUS tiene ventajas y desventajas:

Ventajas

- Facilidad de añadir estaciones de trabajo
- Manejo de grandes anchos de banda
- Muy económica
- Soporta de decenas a centenas de equipos
- Software de fácil manejo
- Sistema de simple manejo

Desventajas

- El tiempo de acceso disminuye según el número de estaciones.
- Cuando el número de equipos es muy grande el tiempo de respuesta es más lento.
- Las distorsiones afectan a toda la red.
- La rotura de cable afecta a muchos usuarios.
- Como hay un solo canal, si este falla, falla toda la red.
- Posible solucionar redundancia.
- El cable central puede convertirse en un cuello de botella en entornos con un tráfico elevado, ya que todas las estaciones de trabajo comparten el mismo cable. Es difícil aislar los problemas de cableado en la red y determinar que estación o segmento de cable los origina, ya que todas las estaciones están en el mismo cable. Una rotura de cable hará caer el sistema.

2.2 Topología Anillo [3] [7][4] [10]

Esencialmente es una red tipo BUS unida en sus extremos. La configuración anillo provee un método alternativo para la transmisión de datos de un computador a otro en un segmento de la red.

El método de transmisión de datos alrededor del anillo se denomina token passing. Esta técnica consiste en que el computador emisor transmite un dato que el computador receptor reciba y que este mande una señal de respuesta informando que recibió el dato correctamente. Todo esto se hace a la velocidad de la luz. Las redes Token Ring no tienen colisiones. Si el anillo acepta el envío anticipado del token, se puede emitir un nuevo token cuando se haya completado la transmisión de la trama. Las redes Token Ring usan un sistema de prioridad sofisticado que permite que determinadas estaciones de alta prioridad designadas por el usuario usen la red con mayor frecuencia. Las tramas Token Ring tienen dos campos que controlan la prioridad, el campo de prioridad y el campo de reserva.

Sólo las estaciones cuya prioridad es igual o superior al valor de prioridad que posee el token pueden tomar ese token. Una vez que se ha tomado el token y éste se ha convertido en una trama de información, sólo las estaciones cuyo valor de prioridad es superior al de la estación transmisora pueden reservar el token para el siguiente paso en la red. El siguiente token generado incluye la mayor prioridad de la estación que realiza la reserva. Las estaciones que elevan el nivel de prioridad de un token deben restablecer la prioridad anterior una vez que se ha completado la transmisión.

Las redes Token Ring usan varios mecanismos para detectar y compensar las fallas de la red. Uno de los mecanismos consiste en seleccionar una estación de la red Token Ring como el monitor activo. Esta estación actúa como una fuente centralizada de información de temporización para otras estaciones del anillo y ejecuta varias funciones de mantenimiento del anillo. Potencialmente cualquier estación de la red puede ser la estación de monitor activo.

Una de las funciones de esta estación es la de eliminar del anillo las tramas que circulan continuamente. Cuando un dispositivo transmisor falla, su trama puede seguir circulando en el

anillo e impedir que otras estaciones transmitan sus propias tramas; esto puede bloquear la red. El monitor activo puede detectar estas tramas, eliminarlas del anillo y generar un nuevo token.

Así como en las redes basadas en BUS, implementación en software y hardware se han desarrollado para eliminar ese tipo de problemas, pero las configuraciones de anillo son más costosas y más difícil de mantener, en comparación con la configuración de BUS. La ventaja de esta configuración, es la de poder transferir en un mismo momento una mayor cantidad de información.

La figura 2.2, grafica la configuración anillo de una red de datos.

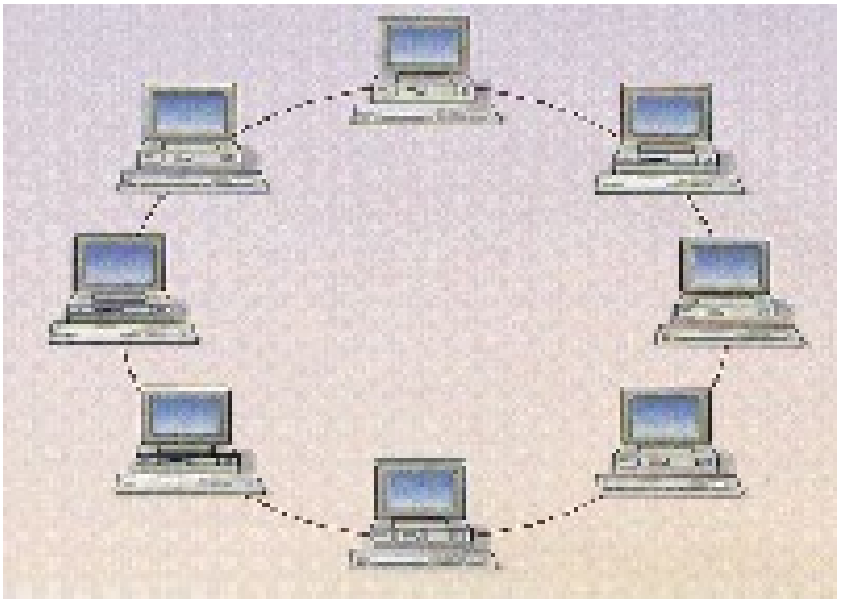


Figura 2.2. Topología Anillo

La topología anillo tiene ventajas y desventajas, destacando:

Ventajas

- El sistema provee un acceso equitativo para todos los computadores.
- El rendimiento no decae cuando muchos usuarios utilizan la red.
- Por ser un sistema de arquitectura sólida, pocas veces entra en conflictos con los usuarios.
- Cada computador funciona como repetidor de la señal, mejorando así la señal.

Desventajas

- La falla de una computadora altera el funcionamiento de toda la red.
- Las distorsiones afectan a toda la red.

2.3 Topología Estrella [3] [7][8] [10]

Todos los cables de los computadores son conectados a un dispositivo central llamado hub (concentrador). Los datos de un computador son transmitidos por el hub al resto de los computadores en red. Esta topología apareció con la utilización del computador mainframe. La ventaja de esta topología es que todos lo procesos son centralizados y esto permite un fácil control de tráfico. Sin embargo, como cada computador tiene que ser conectado al hub, esta topología requiere una gran cantidad de cable para que funcione. Si el hub deja de funcionar, toda la red se detiene. Si un computador sale de funcionamiento, el resto de la red sigue funcionando normalmente.

Este tipo de red es adecuado cuando se tiene un computador central muy poderoso rodeado de máquinas menos potentes que sirven únicamente como terminales de entrada y salida de datos, ya que todos los extremos de la red tienen acceso a los recursos del computador principal de manera directa, sin interferencia de elementos intermedios.

También puede ser usada con redes Punto a Punto, de tal forma que todos los computadores, con iguales características, están conectados al HUB o concentrador y cualquiera de ellos puede tener acceso a los demás. Es una configuración ampliamente utilizada a nivel empresarial.
De esta manera se consiguen enormes velocidades de transferencia de datos, lo que resulta ideal para sistemas que manejen flujos muy grandes de información entre el computador central y sus terminales. Su principal inconveniente es la necesidad de colocar un cable exclusivo para cada terminal.

La figura 2.3, grafica la configuración estrella de una red de datos.

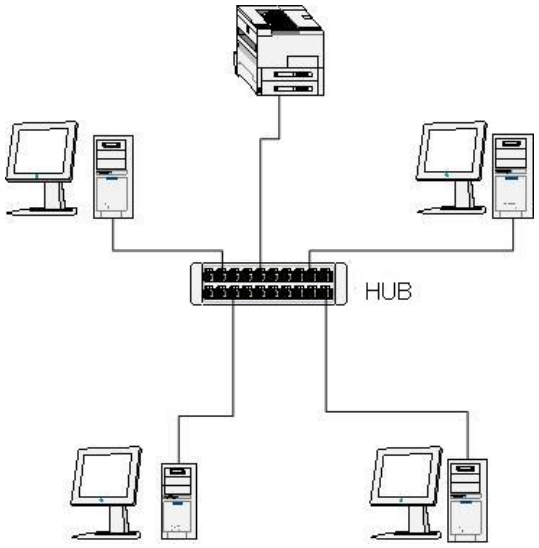


Figura 2.3. Topología Estrella

Ventajas

- Estructura simple.
- Cada PC es independiente de los demás.
- Facilidad para detectar pc's que estén causando problema en la red.
- Fácil conexión a la red.
- Son las mejores para aplicaciones que estén ligadas a gran capacidad de procesamiento.
- Permite añadir nuevos computadores a la red.
- Control de tráfico centralizado.
- La falta de un computador no afecta a la red.

Desventajas

- Limitación en rendimiento y confiabilidad.
- Su funcionamiento depende del servidor central.
- Su crecimiento depende de la capacidad del servidor central.
- La distancia entre las estaciones de trabajo y el servidor.

2.4 Topología Malla (Mesh) [3] [7][8] [10]

Principalmente ofrece redundancia. En esta topología todos los computadores están interconectados entre sí por medio de un tramado de cables. Esta configuración provee redundancia porque si un cable falla hay otros que permiten mantener la comunicación. Esta topología requiere mucho cableado por lo que se la considera muy costosa. Muchas veces esta topología se va a unir a otra topología para formar una topología híbrida.

Las redes en malla son aquellas en las cuales todos los nodos están conectados de forma que no existe una preeminencia de un nodo sobre otros, en cuanto a la concentración del tráfico de comunicaciones.

En muchos casos la malla es complementada por enlaces entre nodos no adyacentes, que se instalan para mejorar las características del trafico.
Este tipo de redes puede organizarse con equipos terminales solamente (en lugar de nodos), para aquellos casos en que se trate de redes de transmisión de datos.

Estas redes permiten en caso de una iteración entre dos nodos o equipos terminales de red, mantener el enlace usando otro camino con lo cual aumenta significativamente la disponibilidad de los enlaces.

La figura 2.4, grafica la configuración malla de una red de datos.

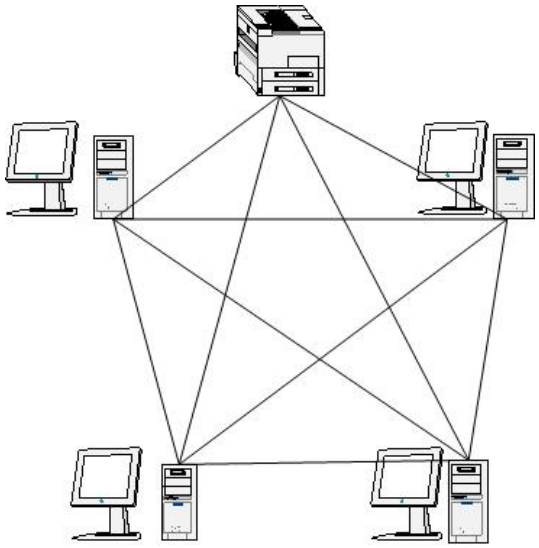


Figura 2.4. Topología MESH

Ventajas

- Por tener redundancia de enlaces presenta la ventaja de posibilitar caminos alternativos para la transmisión de datos y en consecuencia aumenta la confiabilidad de la red.
- Como cada estación esta unida a todas las demás existe independencia respecto de la anterior.
- Control y realización demasiado complejo pero maneja un grado de confiabilidad demasiado aceptable.

Desventajas

- Baja eficiencia de las conexiones o enlaces, debido a la existencia de enlaces redundantes.
- Poco económica debido a la abundancia de cableado.

Existen otro tipo de topologías, las cuales son la mezcla de las ya tratadas, un ejemplo de estas son la topología árbol, la cual es una combinación de subredes de topología estrella conectada a una de tipo bus. Esta nueva topología permite el crecimiento de la red. Otro tipo de red es la que se conoce con el nombre de peer to peer (punto a punto) la cual permite unir dos computadores, con un cable par trenzado configurado como crossover, permitiendo comunicar únicamente a dos computadores.

Los tipos de topologías se resumen en el cuadro 2.1

	Trafico	Vinculo Requerido	Costo	Facilidad de añadir equipos	Desventaja mas importante
Bus	Facil de controlar el trafico en distintos terminales	Fibra óptica porque el trafico es muy importante	No es alto el costo en vinculos ya que utiliza uno a lo largo de la red	Muy facil el nuevo terminal debe "colgarse" del cable simplemente	Depende de un solo vinculo toda la red
Anillo	Las congestiones causada por cableado son dificiles de encontrar	Fibra optica preferentemente	Moderado	Para conectar otro nodo se debe paralizar la red	La falla de un PC altera la red, asi como las distorciones
Estrella	Facil de controlar su trafico, el cual es muy sencillo	El par trensado es aceptable ya que no hay problemas de trafico	Se usa más cantidad de cables y hubs	Depende de la posibilidad del hub (cantidad de puertos)	Se debe usar un cable para cada terminal
Malla	En caso de averias, se orienta el trafico por caminos alternativos	Aunque lo ideal es la fibra optica, el par trenzado es aceptable	Muy alto debido a la redundancia en cableado, bridge, routers	Quizas el mas complicado por la estructura del cableado tan abundante	Poco economica aunque el costo trae beneficios mucho mayores

Tabla 2.1. Resumen Topologías

CAPITULO III
SEGURIDAD

3.1 Definición y concepto de seguridad [4][5][6][7]

Seguridad es proteger información sin importar donde se encuentre (disco o memoria), ni por donde ella viaje en la red.

Hay que tener en cuenta que hay que pensar en que tipo de información es la que se quiere proteger, ¿cuán robusto debe ser el sistema de protección para una situación dada?.

Para que la información sea exacta, confiable y no sea además vista por usuarios no autorizados, hay que seguir cuatro simples reglas de seguridad.

- Integridad: la información es recibida tal como fue enviada.
- Confiabilidad: sin importar cuando fue enviada o recibida, se puede asegurar la integridad de la información.
- Accesibilidad: capacidad de acceder a la información cuando se desee.
- Seguridad: asegurar que la información está protegida de accesos no autorizados.

Hay información que es más importante , por lo cual hay que protegerla más, como identificaciones de usuarios y password. Para saber cuan seguro es un sistema no hay que buscar que protecciones se tienen, sino como podría atacar un intruso. Hay que entender que un ataque no es sólo lo que un hacker, o un craker, pueda hacer en un sistema, sino que puede ser un mal uso del sistema por parte de un usuario inexperto, que por alguna razón cometa algún error y destruya información. Este tipo de ataque se conoce como “ acceso denegado”, por ello un ataque es tan solo una violación de seguridad, integridad o de disponibilidad de información.

La información puede ser definida como un bit o bytes que se trasladan por redes o que se almacenan en ellas. Cuando nos referimos a cualquiera de estos , usualmente nos referimos a ellos como “bienes de información”, los cuales pueden ser un archivo o una base de datos.

En los sistemas informáticos existen seis funciones que son vulnerables a ataques, las cuales son:

- Identificación y autorización: la función identifica usuarios o grupos del sistema.
- Control de acceso: esta función controla y define los derechos de acceso.
- Contabilización: esta función mantiene un seguimiento de la acciones de seguridad más relevantes.
- Objetos reutilizables: esta función previene a un objeto de rehusar recursos como memoria, almacenamiento o comunicación por otro objeto sin la autorización explícita.
- Exactitud o precisión: esta función asegura que los bienes de información se mantienen seguros de sabotajes.
- Fiabilidad del servicio: esta función asegura que la información está disponible.

Hay que tener una buena idea de que se va a proteger, aunque no se sepa como se va hacer eso. Luego hay que determinar cuanta seguridad hay que tener, y eso va en función de la importancia de la información que se desea proteger. La seguridad que se utiliza para contrarrestar una amenaza a los bienes de información, es en algunos casos llamada contramedida, salvaguarda o defensa. Si un ataque es eficaz, se le conoce como *impacto*. Estos impactos son valorados en unidades monetarias, por ello las contramedidas van orientadas a reducir los impactos de los ataques y amenazas. La jerarquización de las estrategias de protección de la información puede ser aplicada a cualquier bien que se desee proteger. Esta jerarquía ayuda a determinar la cantidad de seguridad que se aplicará al problema, de lo más deseable a lo menos deseable, esta lista de jerarquía es la siguiente:

- Evasión o anulación: se aplican medidas de seguridad para evitar ataques o sabotajes, un ejemplo son los firewalls.
- Transferencia: se aplican medidas para transferir la amenaza lejos de los bienes amenazados.
- Reducción de amenazas: se aplica medidas de seguridad para reducir la amenaza. Un ejemplo son las fuentes de poder ininterrumpidas (UPS) que permiten tiempo para que se puedan apagar los servidores de forma correcta.
- Reducción de vulnerabilidad: se aplican medidas de seguridad para reducir la vulnerabilidad de bienes amenazados.

- Detección en tiempo real: se aplican medidas de seguridad para detectar amenazas que están sucediendo en el momento.
- Detección en tiempo no real: se aplican medidas de seguridad para detectar las amenazas que se han realizado a los bienes.
- Reducción de impactos: se aplican medidas de seguridad para reducir el impacto de las amenazas en los bienes, aun cuando sean satisfactorias.
- Recuperación o reposición en tiempo real: se aplican medidas de seguridad para recuperar los bienes que han sido amenazado, por ejemplo duplicidad de disco en un servidor de archivos..
- Recuperación en tiempo no real: se aplican medidas de seguridad para recuperar los bienes pasado un tiempo, por ejemplo un backup.

La seguridad, por lo ya mencionado en la lista, también son las acciones tomadas para mantener los bienes de información seguros. Existen diferentes formas, o métodos, para definir estas acciones o contramedidas. Se pueden realizar evaluaciones de riesgo, para determinar la cantidad y tipo de seguridad que se necesita.

El método de evaluación de riesgos, definiría impactos y amenazas, buscando así las contramedidas adecuadas.

Hay que conocer la naturaleza de las amenazas, ya que así se conocería la forma de como evadirlas, reduciendo las amenazas. Seguridad es, más que todo, **una actitud y filosofa de reglas, políticas, procedimientos y tecnologías.**

Finalmente una definición de seguridad seria, “seguridad es la protección de bienes de información”.

3.1.1 Terminología

Cuando se está hablando de seguridad, se usan términos para identificar ciertas situaciones o acciones. Estas son:

- Vulnerabidades
- Ataques
- Contramedidas
- Amenazas

3.1.1.1 Vulnerabilidades

Los sistemas están desarrollados por Ingenieros, los cuales diseñan e implantan los sistemas a su criterio, conocimientos y conceptos en los lenguajes de programación que utilizan, por lo tanto, es común encontrar errores en los sistemas. Son estos errores los que son usados para tener accesos no autorizados a estos sistemas. Estos errores son los que se han denominado vulnerabilidades.

3.1.1.2 Ataques

Es la forma en la que se usan las vulnerabilidades, se identifican dos tipos de estas, los de extracción pasiva y extracción activa.

En la extracción pasiva, el atacante está atento, escuchando, sin hacer cambios en mensajes ni en la marcha de la red. Este tipo de ataque es difícil de detectar por lo descrito, por ello, si los bienes de información son valiosos o secretos, la única forma de pretejerlos es a través de su encriptación. Un ejemplo de este tipo de ataque, sucede cuando se usan programas llamados SNIFERS, los cuales permiten ver el tráfico de red, y con ello detectar códigos como claves de accesos o identificaciones.

Este tipo de atacante puede identificar:

- El origen y destino de los paquetes de comunicación, así como la información de la cabecera del paquete.
- Monitorear él tráfico y horarios de actividad.

- Identificar el uso de protocolos y observar la transferencia de datos entre los protocolos que no utilicen un sistema de encriptación, como es la versión FTP o Telnet no segura, en las cuales se transfiere la clave en un texto simple de identificar.

En la extracción activa el atacante modifica los mensajes o irrumpe la operación de la red. El atacante tiene como objetivo modificar datos o bien crear tráfico falso. Este tipo de ataque, generalmente puede detectarse, pero no prevenirse. La gama de actividades identificadas sobre ataques conocidos puede clasificarse en cuatro categorías:

1. *Modificación de mensaje*s: al interceptar mensajes, se altera su contenido o su orden para irrumpir su flujo normal.
2. *Degradación y fraude del servicio*: tiene como objetivo intervenir el funcionamiento normal de un servicio, impide el uso o la gestión de recursos en la red. Ejemplo de este ataque es el de negación de servicio (DoS, Denial of Service), donde se suprimen los servicios de SMTP, HTTP, FTP, DNS, entre otros.
3. *Reactuació*n: al interceptar mensajes legítimos, se capturan y repiten para producir efectos diversos, como el ingresar dinero repetidas veces en una cuenta de banco.
4. *Suplantación de identida*d: Este es uno de los ataques más completos y nocivos. El intruso o atacante adopta una identidad con privilegios en una red y explota esos privilegios para sus fines. Un ataque con prioridad de atención para todo administrador de red es el SPOOFING donde el intruso obtiene servicios basados en la autenticación de computadoras por su dirección IP.

Todos estos ataques tienen un impacto relativo a la política de seguridad de un sistema, aunque en Internet dentro de los más temidos se encuentra el DoS por su relevancia al suprimir el funcionamiento de un sistema, y el *Spoofing* al obtener privilegios de acceso de forma fraudulenta.

3.1.1.3 Contramedidas

Lo más importante es contar con una Política de Seguridad, un documento legal y con apoyo directivo, el cual define la misión, visión y objetivos de los recursos de red e información. En una política se define lo que es permitido y lo que no, las necesidades de confidencialidad, autenticación y otros servicios de seguridad para los recursos involucrados. Toda red debe contar con una política de seguridad.

Las contramedidas son políticas de seguridad apoyadas por todos los medios técnicos o de procedimientos que se aplican y desarrollan para atender vulnerabilidades y frustrar ataques específicos. Ejemplos: reglamentos, *firewall*s, ssh, antivirus, kerberos, radius, entre muchos otros comerciales o de dominio público.

3.1.1.4 Amenazas

Las amenazas están dadas por condiciones del entorno, dada una oportunidad y adversarios motivados y capaces de montar ataques que explotan vulnerabilidades, produciéndose una violación a la seguridad (confidencialidad, integridad, disponibilidad y/o uso legítimo). Las posibilidades de amenazas podrían ser, entre muchos:

- Inserción de mensajes solamente.
- Escuchar e introducir mensajes.
- Escuchar y obstruir.
- Escuchar, obstruir e insertar mensajes.
- Escuchar y remitir un mensaje.
- Capacidades activas y pasivas de forma unidireccional o bidireccional.

Cada enlace de una red y cada recurso es susceptible a diferente tipo de amenazas, ataques, y a diferentes atacantes. El análisis de riesgos y el monitoreo constante de vulnerabilidades pueden identificar las amenazas que han de ser contrarrestadas, así como especificar los mecanismos de seguridad necesarios para hacerlo.

Las cuatro categorías generales de amenazas que se utilizan en la actualidad son las siguientes:

1. *Interrupció*n: es una amenaza contra la disponibilidad, el ataque ocasiona que un recurso del sistema deje de estar disponible. Ejemplos: DoS, destruir un elemento de hardware o cortar una línea de comunicación.
2. *Intercepció*n: es una amenaza contra la confidencialidad, el ataque produce la captura no autorizada de información en el medio de transmisión. Ejemplos: *Sniffer*s, lectura de cabeceras, intercepción de datos.
3. *Modificació*n: es una amenaza contra la integridad, el ataque no solo realiza un acceso no autorizado a un recurso, sino también la capacidad de manipularlo. Ejemplos: modificación del contenido de mensajes interceptados, alterar programas para modificar su funcionamiento.
4. *Falsificació*n: es una amenaza contra la autenticidad, el ataque produce que una entidad no autorizada, inserte mensajes falsos en el sistema. Ejemplos: sustitución de usuarios, alterar archivos, inserción de mensajes espurios en la red.

3.2 Niveles de seguridad [2][5]

Las entradas y violaciones de seguridad ocurren a diario, pero no sólo por vándalos en Internet, también sucede físicamente, por uso malicioso de usuarios en los computadores a los que tienen acceso, e incluso, a los que no tienen un acceso autorizado.

La primera institución, o unidad, que se preocupó del tema de la seguridad informática y de sus estándares, fue el Departamento de Defensa de los Estados Unidos; creando un documento, “los criterios de evaluación de estándares verdaderos para computadoras”, Trusted Computer Standards Evaluation Criteria, conocidos cómo el libro naranjo u Orange Book. En el están descritos diferentes tipos de niveles de seguridad que son usados para proteger hardware, software y la información almacenada de ataques. Este documento, describen diferentes tipos de seguridad, como física, de autentificación de usuarios, confiabilidad de los software de sistemas operativos como los de aplicación de usuarios.

Estos estándares, también imponen limites en la intercomunicación entre distintos tipos de sistemas.

Los niveles de seguridad van desde el nivel D, mínima protección, a la A, que es la más segura de todas.

3.2.1 Nivel D1

Este es el nivel más bajo disponible. El sistema operativo es fácilmente comprometido, no hay autentificación, resguardo para los usuarios y para sus derechos de acceso a la información que se almacena es el computador. Este nivel de seguridad se refiere típicamente a sistemas operativos como MS-DOS, MS- Windows, y el sistema 7.x de Apple Macintosh.

Estos sistemas operativos no distinguen usuarios, y no tienen definidos métodos de determinación de quien ingresa información en el computador. Estos sistemas operativos, no tienen sistemas de control de resguardo sobre la información que puede ser accesada en los discos duros del computador.

3.2.2 Nivel C1

El nivel C1, o sistema de protección de seguridad discrecional, describe la seguridad encontrada en un sistema UNIX típico.

Los usuarios deben identificarse al sistema, a través de un nombre de usuario y una clave. Esta combinación es usada para determinar que derechos de accesos tiene cada usuario sobre los programas e información que se encuentre en el computador. Estos derechos de accesos, son los permisos de archivos y directorios. Este control de acceso discrecional, permite que el propietario del archivo o de la carpeta, o el administrador del sistema, prevenga que cierto grupo de personas, puedan tener acceso a programas o información que son de propiedad de ellos. Sin embargo, el sistema de administración de cuentas, no tiene el control de realizar cualquier ejecución de alguna actividad relacionada con las cuentas.

Por ello, cualquier administrador de sistemas inescrupuloso, puede fácilmente comprometer la seguridad, sin que algún usuario se percate de algo.

Agregando a esto, es normal que existan más de un administrador de sistemas, por ello es imposible que se pueda tener seguridad de quién es quién tiene el dominio del sistema. La cuenta del administrador es conocida como ROOT, y el password es común. Por lo ya mencionado, es imposible notar que administrados del sistema ha cometido algún cambio al sistema en si.

3.2.3 Nivel C2

El nivel C2 fue diseñado para ayudar a todas las cuestiones de direcciones. Además de las capacidades del nivel C1, el nivel C2 trae características de seguridad adicionales, que crean ambientes de accesos controlables. Estos ambientes tienen la capacidad de no sólo restringir al usuario de ejecutar ciertos comandos o acceder a ciertos archivos basados no sólo en los permisos, sino que además dependiendo de los niveles de autorización. Estos niveles de accesos requieren que sea revisado el sistema, esto quiere decir, que tienen que ser escritas y revisados los registros para cada evento que ocurre en el sistema.

La revisión se utiliza para guardar los expedientes de toda la seguridad relacionada con eventos, como las actividades desarrolladas por el administrador. La revisión requiere de una autentificación adicional, debido a que sin ella, no se podría estar seguro que una persona que ejecute los comandos sea ella o no. La desventaja de la revisión, es que requiere de recursos adicionales del subsistema del procesador y disco.

Con el uso de autorizaciones adicionales, es posible para usuarios en el sistema C2, puedan tener la autoridad para realizar tareas administrativas en el sistema sin tener la contraseña del ROOT.

Esto permite que mejore las tareas de administración, ya que esto permite que un usuario individual realice su trabajo sin que el administrador del sistema tenga que intervenir.

Estas autorizaciones adicionales no pueden ser confundidas con los permisos SGID y SUID, que son aplicados a los programas. Sin embargo, hay autorizaciones que permiten al usuario ejecutar comandos específicos o acceder a ciertas tablas del núcleo (kernel) del sistema. Los usuarios que no tienen las autorizaciones apropiadas para ver las tablas de procesos, por ejemplo, solo pueden observar sus procesos cuando ejecutan el comando *ps* de UNIX.

3.2.4 Nivel B1

El nivel B1, o Protección Etiquetada de Seguridad, es el primer nivel que apoya la seguridad de multi-nivel, tal como secreto y súper secreto. Este nivel no permiten que los permisos de un archivo puedan ser cambiados por el usuario propietario del archivo, solo puede ser cambiado por el ROOT (administrador del sistema operativo).

3.2.5 Nivel B2

El nivel B2, conocido como protección estructurada, requiere que cada objeto esté etiquetado. Los dispositivos como discos, cintas, o terminales pueden tener un solo nivel o un multi-nivel asignado a ellos. Éste es el primer nivel que comienza a tratar el problema de un objeto en un nivel más alto de seguridad que se comunica con otro objeto en un nivel inferior de seguridad. Se consolidad mecanismos de autentificación. El sistema es relativamente resistente a la penetración de un atacante.

3.2.6 Nivel B3

El nivel B3, o nivel de seguridad de dominios, hace cumplir el dominio con la instalación del hardware. Por ejemplo, el hardware de administración de la memoria, se utiliza para proteger el dominio de seguridad contra el acceso o la modificación desautorizada de objetos en diversos dominios de seguridad. Este nivel también requiere que el terminal esté conectado con el sistema a través de una ruta confiable.

Este nivel los requerimientos de monitoreo de referencia que media todos los accesos relacionados a objetos, que son sujetas a análisis y pruebas. La estructura de seguridad excluye códigos no esenciales a las aplicaciones de seguridad.

3.2.7 Nivel A

El nivel A, o nivel verificado de diseño, es actualmente el nivel más alto de la seguridad validado por el Orange Book. Incluye un diseño riguroso, un control y verificación de los procesos.

Para que este nivel de seguridad sea alcanzado, todos los componentes de los niveles más bajos tiene que ser incluidos (niveles D a B3); el diseño tiene que ser verificado matemáticamente, y un análisis de canales cubiertos y de distribución debe ser realizada. Distribución verificada significa que el hardware y software tiene que ser protegidos durante su distribución para prevenir manipulación indebida de los sistemas de seguridad.

3.3 Seguridad Física y Personal [6]

La seguridad , como se explico al comienzo del capitulo, se refiere a todos aquellos mecanismos dirigidos a que no se viole el sistema informático que almacena bienes de información, como a su vez su resguardo de accidentes que dañen la integridad física del sistema informático. Este tipo de seguridad se puede dividir en dos tipos de seguridad la física y la personal.

3.3.1 Seguridad Física

Aquí se refiere a la implementación de medidas que protejan físicamente los sistemas informáticos contra accidentes o fenómenos naturales que afecten la integridad física de los sistemas informáticos, como también, su funcionamiento en el tiempo. Todo esto se logra con la implementación de equipos que detectan humo e incendios, protecciones eléctricas contra sobre tensiones, sistemas UPS, grupos electrógenos, instalaciones de protección a tierra que tengan menos de 0,8 V. Este último punto es muy importante, ya que si ocurre algún accidente con el sistema eléctrico, la instalación a tierra, desviaría la sobre tensión que se pueda producir y dañar a los equipos informáticos. Existen otros elementos que pueden producir problemas o destruir los sistemas informáticos, ellos son producidos por condiciones del medio ambiente, como la temperatura, la pureza y humedad ambiente, por ello es que se implementan sistemas de aire acondicionados en las salas que albergan los sistemas informáticos. Por la cantidad de energía

eléctrica utilizada, es de mucha importancia la puesta de puntos de tierras ya mencionados, esto porque se crea electricidad estática, la que también es conducida por los puntos a tierra.

El problema de la implementación de estos sistemas, es el gran costo de ellos, por lo que muchas veces no se implementan estas medidas, produciéndose pérdidas materiales al producirse alguno de los accidentes ya nombrados.

No hay que olvidar, que los fenómenos naturales también podrían destruir o interrumpir un sistema informático, una inundación, huracán o un terremoto, pueden dañar o destruir las instalaciones donde se instalan los sistemas, por ello , hay que diseñar instalaciones que cumplan las medidas de seguridad que prevengan algún tipo de daño a los sistemas informáticos.

3.3.2 Seguridad Personal [2][4][5][6]

Cuando se está diseñando un sistema informático, además de prever las exigencias que involucran la seguridad física, hay que prever otro tipo de seguridad, que tiene que ver con la seguridad que impide o entorpece el acceso físico de alguna persona a las instalaciones donde se encuentre instalado el sistema informático. Para ello se diseñan puertas con llaves especiales, mecanismos electrónicos de apertura por claves secretas, huellas digitales, reconocimiento de retina, voz, etc.

3.4 Seguridad Lógica [6][7][8][9]

Cuando ya se han implementado sistemas de seguridad físicos y personal, el riesgo a que personas no autorizadas dañen los sistemas son mínimos. Sin embargo, hay que implementar sistemas de seguridad en los sistemas informáticos, para que un usuario del sistema , o algún individuo que transgreda la seguridad física, no pueda manipular la información contenida en el mismo, para la cual no estén autorizados.

Este tipo de seguridad se conoce como seguridad lógica o de capas, esta es mucho más efectiva que la seguridad que se aplica a una contramedida, ya que si se tiene una contramedida de seguridad, su violación es más fácil, en comparación a una de varias capas.

La seguridad por capas logra dos cosas; primero coloca barreras repetidamente, controles y otras medidas entre el atacante y los bienes de información. De esta forma se mitiga la vulnerabilidad del sistema, de esa forma si es violada una capa, existen más capas que protegen el sistema.

Este sistema funciona de la siguiente manera:

“ Si un usuario desea entrar al sistema, tiene que ingresar una identificación de usuario y una palabra secreta (clave) que le da acceso al sistema (primera capa), al cual está autorizado a ingresar. Si quiere hacer uso de una aplicación (software) debe ingresar otra clave (segunda capa), y finalmente , solo se puede acceder al directorio que contiene un archivo si es que se encuentra autorizado (tercera capa). Se puede agregar otra capa de seguridad, encriptando los archivos de las carpetas. De esa forma, si un intruso llega a pasar las capas, solo podrá encontrar solo un archivo que no tendría ningún sentido.” [5]

La segunda cosa que se logra con las capas, es la conveniencia del usuario. Si se implementan correctamente las capas, el legítimo usuario no tendrá dificultad de acceder a la información a la cual está autorizado. Esto ejemplifica otro aspecto de la seguridad que no se aludió, la conveniencia.

Existe otra forma de tener seguridad lógica, esta es a través de la segmentación de la red en redes virtuales, a través de la implementación de subredes, las cuales se logran configurando los routers de entrada que se encuentran en cada subred. En estos routers se pueden implementar filtros, que solo permitan la entrada y salida de algunos IP de la red propietaria, u de otras redes, siendo más difícil la violación de los sistemas informáticos que se encuentran dentro de estas redes. También se pueden implementar filtros según los puertos a los que se quieran acceder.

3.5 Reconocimiento de Riesgos en Administración [6]

Para el reconocimiento de riesgos en la administración de la seguridad considera las políticas de seguridad.

La declaración de política de seguridad, es una declaración formal de reglas por las cuales las personas que tienen acceso a la tecnología y bienes de información de la organización, deben seguir y respetar.

Las políticas deben ser propuestas por los principales representantes de la corporación, como los miembros de administración, que tiene el presupuesto, y la autoridad política, los miembros técnicos que saben que puede ser o no implementado y el personal legal, que tienen el conocimiento de las ramificación de las elecciones de las políticas de seguridad.

Los beneficios que implica la formulación de políticas de seguridad son:

- Proveer un marco para implementar los aspectos de seguridad de la infraestructura de la red.
- Proveer el proceso por el cual se puede auditar la existente red de seguridad.
- Identificar los procedimientos que son considerados convenientes, prudentes, ventajoso y productivos.
- Habilitar la implementación u ejecución de seguridad global.
- Crear las bases de las acciones legales necesarias.

Una política de seguridad exitosa debe ser llevada al papel y demostrar que han sido bien pensadas. Los siguientes puntos son características importantes de una buena política de seguridad:

- Deben ser capaces de ser implementadas técnicamente.
- Deben ser capaces de ser implementadas organizacionalmente.
- Deben ser ejecutadas con herramientas de seguridad cuando sea apropiado y con sanciones donde la prevención no sea técnicamente factible.
- Deben definir claramente las áreas de responsabilidad de los usuarios y administradores.

- Deben ser flexibles y adaptables para los ambientes cambiantes.

Una política de seguridad no debe determinar como una organización debe operar; la naturaleza de la organización dicta la política de seguridad. Definir la política de seguridad de una organización puede resultar difícil de definir, pero definiéndola antes de elegir métodos de seguridad, las organizaciones pueden evitar el rediseño de las metodologías después de implementarlas.

Un punto que debe tomar en cuenta una organización, al generar una política de seguridad, es el compromiso por parte de los integrantes que la componen. Este compromiso puede ser tomado de diferentes formas, siendo en el caso de las empresas, oficinas gobernamentales, la firma de cláusulas de responsabilidad profesional, responsabilidad legal, conflictos de intereses y confidencialidad. Si un miembro de la organización no cumple con estas cláusulas, las organizaciones pueden tomar acciones legales en contra de los miembros que han faltado a ellas. Es importante definir bien los deberes, acciones y compromisos de los miembros, entregándoles a ellos, un manual donde se explique su acción frente a problemas de seguridad, frente a la información que manejen antes y después que formen parte de la organización. Un ejemplo, es si se hiciera la pregunta “¿utiliza la organización algún tipo de firewall?”, responder que no se sabe o que no se usa, ya que de esa manera , un hacker manejaría información que le ayudaría a comenzar un ataque contra los sistemas de información de la organización. Otro ejemplo sería la posibilidad de no poder copiar información de los sistemas de información de la organización para ser usada, procesada o leída fuera de las instalaciones de la organización. La oportunidad hace la ocasión, por ello, hay que tratar de que se tengan las reglas claras por parte de los miembros de la organización desde un principio.

3.5.1 Administración de riesgos

La administración de riesgo es una aproximación sistemática para determinar las medidas apropiadas de la seguridad de las organizaciones y de su mantenimiento.

Antes de que las redes informáticas crecieran, la información confidencial era mantenida bajo llave, y eran confiadas a las personas el mantener la información confidencial en lugares seguros.

En el pasado existían medidas de seguridad muy distinta a las existentes en la actualidad; un ejemplo es el del Departamento de Defensa de Estados Unidos (DoD). En los accesos del DoD existen agentes de seguridad, los cuales revisaban maletines y carteras cada vez que alguien ingresaba o salía de las instalaciones, no se podía abandonar el edificio sin ningún medio magnético o documentos impresos, los cuales eran impresos en papel de otro color.

En los ambientes actuales, todas esas medidas de seguridad son obsoletas, debido a que existen las redes informáticas. En la actualidad, se puede encriptar la información y enviarse por correo electrónico. Las redes informáticas han creado un ambiente donde la información puede ser accedida, movida o destruida electrónicamente.

3.5.1.1 Evaluación de riesgos

La evaluación de riesgos va dirigida a la combinación de la identificación de bienes, la valorización del bien y la determinación de probabilidades de brechas de seguridad. Cuando ya se han identificado los recursos críticos (bienes) y la probabilidad con el costo asociado con el compromiso de destrucción, y la inaccesibilidad del recurso crítico ha sido valorado, se puede tomar la decisión de que nivel de riesgo es aceptable para la organización, y es única para esta debido a que las necesidades de la organización, la confiabilidad de los usuarios y la localización de los bienes son diferentes en cada organización.

3.5.1.1.1 Identificación de bienes de la red

No es conocido el tipo de enemigo potencial de las organizaciones, por ello , se tiene que tener claro y conocer muy bien la organización. Las organizaciones tienen que saber que desean proteger, que accesos se necesitan para acceder a esos bienes, y como deben interactuar estos dos puntos. Se debe estar más preocupado de los bienes y los valores asociados, más que a la motivación de un atacante.

Se debe identificar que se va a proteger. Algunos puntos a considerar son los de la tabla 3.1.

Bienes	Descripción
Hardware	Estaciones de trabajo, computadores personales, impresoras, routers, switches, modems, terminales, servidores, firewalls, etc.
Software	Programas fuentes, utilidades, programas de diagnostico, sistemas operativos, programas de comunicaciones, etc.
Datos	Almacenamiento en tiempo real de datos y no tiempo real, respaldos, registros de auditoria, bases de datos, datos en transito en medios comunicación, etc.
Personal	Usuarios, administrador, encargados de mantención de equipos.
Documentación	Programas de software, hardware interno y software de evaluación, sistemas y procedimientos administrativos locales, procedimientos de seguridad.

Tabla 3.1. Identificación de Bienes

3.5.1.1.2 Valorización de los bienes

Es un proceso subjetivo el valorar un bien de una organización. Los bienes tangibles se pueden valorar según el precio de su reemplazo, mientras que los bienes intangibles, como software desarrollado, documentación o datos, tienen una valorización en términos de importancia o de decisividad. La pérdida de estos últimos, es más importante que el valor que este tenga.

El reemplazo de un bien, puede bordear al costo de adquisición de elemento físicos de seguridad, (firewalls, dispositivos de encriptación, etc), como también el entrenamiento del personal en su uso. La pérdida de información es el impacto inmediato de la corrupción de datos , pueden hacer que se llegue a plazos límites en la entrega de proyectos, documentos, o cualquier otro proceso que involucre cumplir con estos tiempos. En muchos casos la estimación del valor de los datos es difícil, especialmente cuando se está en ambientes de investigación donde se encuentran cambios en el ambiente de la organización. Se puede estimar que una informaciones muy importante, ya que esta puede ser la base de una patente de muchos millones de unidades monetarias.

Clasificar los datos de acuerdo una variedad de niveles de criticalidad puede ser el paso preliminar al establecer su valor. Un ranking simple puede ser de **alto**, **medio** y **bajo**, y es el comienzo de la evaluación de la criticalidad de una información. Los datos puede tomar diferentes formas, incluyendo las siguientes:

- Datos Administrativos.
- Datos Financieros.
- Datos de Clientes.
- Datos de Investigación.
- Datos Propietarios (datos que no son de uso público y son propietaria de un usuario).

Un ejemplo de esto es la descrita en la tabla 3.2.

Tipo de datos	**Clasificación**	**Criticalidad**
Resultados de ensayos clínicos	Investigación	Alta
Tendencia de mercados	Investigación	Baja
Patentes pendientes	Propiedad	Alta
Memos corporativos	Administrativo	Baja
Archivos de localización de empleados	Administrativo	Baja
Nuevo desarrollo de productos	Propietario	Media
Tendencia de Secretos	Propietario	Alta
Datos de adquisición	Financiero	Alta
Salarios de empleados	financiero	Media

Tabla 3.2. Ejemplo Prioridades

3.5.1.2 Vulnerabilidades y Ataques

Una vez que se han identificado los bienes de información, se debe determinar los posibles ataques a ellos, y las probabilidades de la vulnerabilidad de estos ante un ataque.

Un ataque puede ser una persona, objeto, o un evento que potencialmente pueda causar daño a la red o a los dispositivos de ella. Los ataques pueden ser intencionales o accidentales.

Una vulnerabilidad es una debilidad en la red que puede ser explotada por un ataque. Por ejemplo, un acceso no autorizado (ataque) a la red puede ser realizado por un usuario externo a la red, adivinando una clave de acceso (password) que sea común. La vulnerabilidad en este caso, es la clave de acceso tan común que fue elegida por el usuario.

La reducción, o eliminación de los aspectos vulnerables de una red, puede reducir o eliminar el riesgo de ataques a la red.

Los ataques pueden ser, usualmente, identificados de la siguiente manera:

- Espionaje o robo de información
- Deshabilitación de acceso a los recursos de la red (ataque de denegación de servicios, DoS)
- Acceso no autorizado a los recursos
- Manipulación de datos

Si estos ataques son realizados, y los dispositivos o datos son comprometidos, existe una gran posibilidad de pérdidas cuantiosas en unidades monetarias, por lo que fuertes medidas de seguridad deben ser implementadas.

Algunos impactos de ataques pueden tener como consecuencia el compromiso de datos, pérdida de la integridad de los datos y la indisponibilidad de los recursos de la red.

a) Compromiso de datos

Toda información almacenada o transferida electrónicamente puede ser potencialmente robada. Un intruso que tiene acceso no autorizado a un sistema, o que pueda espiar, intercambios de información confidencial, puede apoderarse de la información y divulgarla. Dependiendo del tipo de información divulgada, el resultado puede ser intranscendente a catastrófica, por ello se crea una lista de prioridad que debe ser evaluada por la organización.

Datos pertenecientes a información de consumidores, datos del personal, datos financieros, son siempre extremadamente sensible y por ello, valiosos.

b) Pérdida de integridad de información

La pérdida de la integridad de la información es extremadamente costosa por las organizaciones. La perdida de ellas, se traduciría en la pérdida de la credibilidad de la organización, y por ende, de ingresos.

El costo de investigar la pérdida de integridad de la información es muy alta. Debido a que las organizaciones tienen que mantener su información al día, no se puede mantener la información alterada, esto ya que se recupera la información de los respaldos (backup) si es que existen. Después de recuperar la información hay que investigar la forma como fue comprometida la información, para poder determinar, donde y como la información fue comprometida.

Cuando se determinan posibles riesgos de seguridad, la organización debe considerarla para poder evitarlos. Actualmente, la información de las organizaciones es almacenada en medios magnéticos, por lo que si no se crean respaldos continuamente, y no se toman medidas de protección de los computadores, pueden colapsar y perder la información. Una política de seguridad clara debe ser propuesta para preservar la integridad de la información.

c) Inaccesibilidad de recursos

Cuando un recurso de la red llega a estar inaccesible, el resultado en pérdidas pueden ser cuantiosas. En estos días, son más las organizaciones que trabajan sus transacciones a través de redes informáticas, y la inaccesibilidad a los sistemas son críticos, contabilizándose en millones de unidades monetarias.

Se tienen que estimar el costo del tiempo fuera de servicio de los sistemas, causados por fallas de los sistemas, de fenómenos naturales, o por ataques. Los recursos de un sistema pueden ser inalcanzables por configuraciones defectuosas o por planes inadecuados de actualización de software.

3.5.1.4 Evaluación de riesgos

Por la variedad de los posibles ataques, hay que evaluar riesgos. Existen muchas metodologías para medir el riesgo. Comúnmente, se define el riesgo en términos cuantitativos, cualitativos o ambos. La evaluación de riesgo cuantitativo usa datos empíricos, probabilidades y estadísticas conocidas. El análisis cualitativo usa valorización intuitiva. Sin importar la forma que

se use, el aspecto importante es como cuantificar la cantidad perdida y la probabilidad que ocurra debe ser consistente con el significado que las personas que toman las decisiones acerca de como protegerse de los riesgos.

Una forma simple de calcular el riesgo es calculando la probabilidad relativa que un ataque ocurra y el valor esperado de las pérdidas, como se observa en la tabla 3.3.

Probabilidad de ataque (Ap)	Pérdida prevista (Pp)	Riesgo (Ap*Pp)
1= Menos Probable	1= Baja Pérdida	1,2= Bajo Riesgo
2= Presuntamente Probable	2= Pérdida Moderada	3,4= Riesgo Moderado
3= Muy Probable	3= Pérdida Critica	6,9= Alto Riesgo

Ap	Pp	Riesgo
1	1	1→ bajo
1	2	2→ bajo
1	3	3→ moderado
2	1	2→ bajo
2	2	4→ moderado
2	3	6→ alto
3	1	3→ moderado
3	2	6→ alto
3	3	9→ alto

Tabla 3.3. Calculo de Riesgo

Se pueden encontrar el riesgo de otra forma más específica de la siguiente forma:

Tomando como ejemplo una red de una empresa de ventas de insumos electrónicos, la tabla 3.4 determina cuan críticas son las consideraciones de seguridad de cada red, usando una

combinación de importancia de la red, la probabilidad de sucesos nocivos, probabilidades de degradación del rendimiento de la red después que un suceso nocivo le afecte.

LAN	D	I	C	IR	PA	PD	RR
Administración	2	3	1	6	Muy bajo 0.1	Bajo 0.3	3.8
Ingeniería	2	3	2	12	Moderado 0.5	Moderado 0.5	2.0
Finanzas	2	3	3	18	Bajo 0.3	Bajo 0.3	8.8

Tabla 3.4. Evaluación Riesgo

1. D = disponibilidad I = Integridad C = Confidencialidad
2. IR = Importancia de la red. IR = D*I*C
3. PA = Probabilidad de acontecimiento. Es determinado por la consideración del número de usuarios, acreditación previa, frecuencia de respaldos, y requerimientos de protecciones obligatorias y no obligatorias.
4. PD = Prevención de degradación. La capacidad de PD de D, I, C para una red en la situación de un suceso nocivo, es determinado usando la necesidad relativa de proteger la disponibilidad, integridad, sensibilidad de los datos y la criticidad de la capacidad de procesamiento de datos.
5. RR = Riesgo relativo. RR = IR*[(1*PA)*(1-PD)]

IR es la importancia de la red.

1*PA es proporcional a la probabilidad que el rendimiento de la red se degrada después de que se inicio un evento.

En la tabla 3.4, en la columna izquierda, se identifica la red a evaluar. La columna IR establece la importancia relativa de cada red. Los valores en las columnas PA y PD están determinados usando una clasificación cualitativa (muy bajo, bajo, moderado, alto, muy alto) y de la siguiente escala:

Muy bajo	0.1
Bajo	0.3
Moderado	0.5
Alto	0.7
Muy Alto	0.9

Para los administradores de una red, el establecer la importancia de ella es importante, debido a que facilita la asignación de recursos para proteger los bienes que son parte de la red.
Importancia de red, es un término usado para describir la relativa importancia de una red con la consideración de las demás redes de la organización.

El cálculo del riesgo relativo RR, proporciona al administrador de información que le indica el rango de riesgo asociado en las redes de la organización. Este ranking de importancia de las redes facilita la asignación de recursos para la implementación de protecciones adicionales.

Hay que notar que la magnitud de la diferencia de RR entre varias redes no es importante. El número reflejado en la columna derecha de la tabla 3.4 representa el riesgo relativo, entre mayor sea el valor, mayor es el riesgo relativo. La red, con el mayor valor representa el mayor riesgo relativo de la organización.
En el ejemplo de la tabla 3.4 , el red del área financiera es la que tiene mayor importancia, por lo cual es a esa red a la cual hay que implementar un sistema de seguridad mayor que a la red de ingeniería.

CAPITULO IV
METODOS DE ESPIONAJE

4.1 Scanners [5]

Programas que automáticamente detecta las debilidades de seguridad de una computadora.

Los verdaderos scanners, son exploradores de puertos TCP, esto a través de ataques a los puertos TCP/IP y los servicios (por ejemplo telnet o ftp), almacenan la respuesta obtenida del computador destino. De esta forma se recaba información valiosa de la computadora de destino.

Existe otro tipo de aplicaciones para de redes, del sistema operativo Unix, que se conocen con ese nombre. Esta aplicación no es realmente un scanner, pero recolecta información de ciertos servicios que trabajan en otras maquinas.

Los scanners se han diseñado para diferentes plataformas de sistemas operativos, encontrándose algunos como PortScanners, de Cyberkit, y Nmap, original de Unix, pero diseñado para su uso en Windows en formato de línea de comando.

Para correr estas aplicaciones, deben de ser compatibles con la plataforma operativa que se utiliza en el computador. Además se tiene que contar con una computadora que cuente con bastante memoria ram, procesador, y una buena conexión a Internet, banda ancha es lo recomendado.

Los scanners no son de uso ilegal, ya que son diseñados y distribuidos por desarrolladores y personal de seguridad. Son software de uso público, permitiendo que un usuario, o administrador de red, pueda encontrar sus propias debilidades.

4.1.1 Atributos de un scanner

Los atributos primarios de un scanner son:

- Capacidad de encontrar una computadora o una red.
- Capacidad de encontrar que servicios están siendo usados en la computadora.
- Capacidad de prueba de los servicios, en búsqueda de un agujero en un sistema.

4.2 Password Crackers [5]

Es un programa que pueden descifrar, o deshabilitar la protección de password de algún software. Este tipo de programas no pueden descifrar cualquier password, de hecho, passwords encriptados no pueden ser descifrados. Las técnicas modernas de encriptación solo permiten la encriptación, y no la reversa de esta. Por ello, no se pueden obtener los passwords, obligando a los administradores de las redes a entregar, cambiar, nuevas passwords en el caso de la perdida de ella.

Se utilizan herramientas (softwares) de simulación, utilizando algunos algoritmos de los programas generadores de passwords originales. A través de un análisis comparativo, estas herramientas tratan de buscar la correspondencia entre la versión encriptada de un password y la original, que es la entrada a un sistema. El problema que se encuentra es la pereza de los usuarios a usar un password, o la de que un password son palabras simples, que se encuentran en cualquier diccionario.

4.2.1 Funcionamiento de un Password Crack

Para comprender como trabaja un password crack, hay que entender como trabaja un generador de passwords. La mayoría de los generadores utilizan criptografía. La palabra criptografía proviene del griego, de la palabra Kyptos, la cual es usada para describir algo que es escondido, opacado, encubierto, secreto. La palabra grafía proviene de gráfica, y significa escrito. Por lo tanto, criptografía es el arte de la escritura secreta. Otra definición a sido dada por Yaman Akdeniz, en su publicación , Criptografía y Encripción, de 1996, donde sita:

“ Criptografía se define como la ciencia y estudio de la escritura secreta , concerniente a la forma en que la comunicación y datos pueden ser codificados para prevenir la revelación de su contenido a través del espionaje o la intercepción de mensajes, usando códigos, codificación u otros métodos, siendo solo algunas personas las que puedan ver el mensaje real”[5].

Un ejemplo de criptografía es el crear un código, donde cada letra del alfabeto corresponda a un numero u a otra letra. La figura 4.1 se indica el código ROT-13. este método se forma con la correspondencia de una letra del alfabeto. Este código trabaja sustituyendo una letra con la que esta a 13 letras más adelante en el alfabeto. Esto es una simple sustitución.

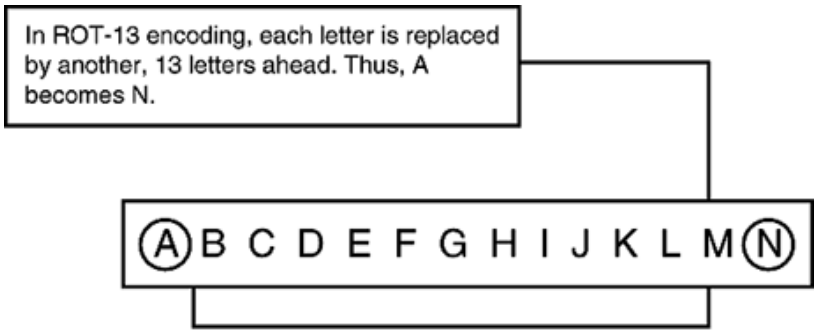


Figura 4.1. Método ROT-13

Cualquier forma de encriptación es útil, dadas circunstancias particulares. Estas circunstancias dependen del tiempo, la sensibilidad de la información, y de quien se trata de ocultar la información.

4.3 Troyanos [5]

Conocido también con el nombre de “ Caballo de Troya”, es un programa que se confunde con otros códigos maliciosos. Un troyano es:

- Un programa no autorizado, contenido en un programa legitimo. Este programa no autorizado ejecuta funciones desconocidas y no deseadas por el usuario.
- Un programa legítimo, que ha sido alterado por la inserción de un código desautorizado en él, este código ejecuta funciones desconocidas y no deseadas por el usuario.

- Cualquier programa que aparece ejecutando una función necesaria y deseada, pero que ejecuta funciones desconocidas, o no deseadas, por el usuario, por contener un código desautorizado, que no es conocido por el usuario.

Funciones no autorizadas que el troyano ejecuta, algunas veces clasifican en otro tipo de dispositivo malicioso. Algunos virus se amoldan a esta categoría.

Documentos clásicos de seguridad en Internet lo define de varias formas. La definición mas conocida es la entregada en el RFC 1244, Site Security Handbook:

“ Un caballo de Troya puede ser un programa que hace algo útil, o simplemente algo interesante. Siempre hace algo inesperado, como robar las contraseñas (passwords), o copiar sin que se sepa”.

Otra definición que es adecuada, es la dada por el doctor Alan Solomon, especialista de renombre internacional, en su trabajo “ Todo acerca de virus” (All about viruses):

“ Un troyano es un programa que realiza algo más de lo que un usuario espera, y esta función extra es la perjudicial. Esto lleva al problema en la detección de troyanos”.
Analizando las definiciones entregadas, se puede concluir que, un troyano es un programa que realiza una función oculta indeseada. Esta función puede venir en cualquier forma, pudiendo venir en cualquier programa que corran los usuarios.

4.3.1 Origen de los troyanos

El termino troyano fue adquirido debido a la similitud de la forma como son ocultos los códigos maliciosos dentro de otro código mayor y la historia de Grecia, la invasión de la ciudad de Troya.

Los troyanos son creados a través de un cronograma, que puede cumplir con cualquier cosa, pero un troyano realizará al menos una o dos acciones:

- Ejecutar alguna función que revela al programador información vital y privilegiada de un sistema o compromete al sistema.
- Ocultar alguna función que revela al programador información vital y privilegiada de un sistema o que compromete al sistema.

Algunos Troyanos realizan ambas acciones. Además de las acciones descritas, existen otras acciones que pueden realizar, como encriptar o formatear un disco duro.

Sin embrago, los Troyanos han sido insertados por individuos que están relacionados con el desarrollo legitimo de los sistemas. Estos son trabajos internos, donde algunos desarrolladores de software, insertan códigos no autorizados en la aplicación o utilidad. Esto puede llegar a ser más peligroso por varias razones:

- Estos troyanos no son destructivos, recolectan información en los sistemas. Su descubrimiento es tardío, hasta que es revelado por accidente.
- Ya que la mayoría de los servidores usan el sistema operativo Linux, algunos sitios muy confiables, pueden ser comprometidos, obteniéndose los passwords de los usuarios del sistema.
- Los troyanos se pueden encontrar un software descargado desde Internet, especialmente en sharewares o freewares. También en material descargado de servidores clandestinos (kazza, i-mesh, etc).

4.3.2 Nivel de riesgo que representa un Troyano

Los Troyanos representan un alto nivel de riesgo, por diferentes razones:

- Son de difícil detección
- Se encuentran en código ejecutable
- Pueden afectar a muchas maquinas

Los Troyanos son el perfecto ejemplo del tipo de ataque que es fatal para el administrador de un sistema que tiene un bajo nivel de conocimiento en seguridad. Un troyano puede comprender la totalidad de un sistema.

El troyano puede estar oculto por un largo tiempo, hasta que se active o sea descubierto.

4.3.3 Detección de un Troyano

Una forma de detección es por medio de antivirus actualizados, además del uso de Firewalls, que detecten tráfico no autorizado, causando por algunos Troyanos. Otra forma de detección es por medio de la técnica conocida como "unificación de objeto". Esta técnica consiste en comparar objetos (archivos) con copias de los mismos respaldos anteriores. Se compara, en primera instancia el tamaño, fecha y hora de modificación de los objetos. De encontrar algo sospechoso, se procede a la comparación de la información.

4.4 Sniffers [5][6][15][13]

Sniffer es un software que recolecta toda la información que se desplaza por un segmento de red, recolectando paquetes de información en cualquier protocolo (Ethernet, TCP/IP, IPX, etc).

Un equipo con el software de tipo Sniffer, puede ser instalado en algún punto de la red, a través de una tarjeta de red, u otro dispositivo de comunicaciones, configurando el software al dispositivo de comunicaciones en modo promiscuo.

Modo promiscuo, es la configuración o modo en que la tarjeta de red , o el dispositivo de comunicación, escucha (recolecta) todo el tráfico del segmento de la red. Este software no se debe confundir con los softwares conocidos como *keylog*, los cuales son usados para grabar la secuencia de teclas presionadas en el teclado usando en alguna máquina.

Debido a que la información viaja a una máquina del segmento de red, se genera un broadcast a cada máquina del segmento de red. Eso significa que cada máquina recibe y ve la información que tiene por destino a otra maquina del segmento, pero la ignora, a menos que se le instruya lo contrario. Entendiendo lo anterior, se entiende la forma como trabaja un Sniffer. Le dice a la

máquina, puntualmente a la tarjeta interfase de red (NIC), que pare de ignorar todo el tráfico dirigido a otras máquinas y que pongan atención en ellas. Para que la NIC se configure en *modo promiscuo*, se requiere tener privilegios de administrador o de root. Luego, el programa comienza a leer constantemente toda la información que pasa a través del dispositivo de comunicación de la máquina. La información se transporta en tramas o paquetes, y es desarmada en sus específicos protocolos. Debido al formato de los protocolos, un Sniffer puede descomponer las capas de encapsulación y decodificar información revelante almacenada en ellas, dirección de origen, dirección de destino, número de puerto apuntado, etc.

4.4.1 Nivel de riesgo que representan los Sniffers

En una red LAN, existen paquetes que se intercambian entre múltiples máquinas cada minuto, ampliando la fuente de cualquier ataque.

Cualquier texto transmitido a través de la red será vulnerable, contraseñas, páginas web, petición de información de una base de datos, por nombrar algunas.

Un Sniffer puede personalizarse para capturar un tráfico específico, como sesiones de telnet o e-mail. Una vez que se ha capturado un tráfico, un cracker puede extraer rápidamente información que necesite, como identificaciones, claves o textos de mensajes. El usuario nunca se enteraría que ha sido víctima de la intercepción de sus datos. Los Sniffers no causan daño o perturbación en el entorno.

4.4.2 Detección y anulación del uso de Sniffer

Para evitar el ataque o uso de un Sniffer en un segmento de red, es necesario el diseño de una topología segura de red, lo cual significa, que no existan puntos físicos donde se pueda conectar un cracker. Esto implica un alto desembolso de recursos en la implementación de la red.

Para poder anular el ataque de este tipo, hay que implementar algunas reglas.

- Los segmentos de red solo pueden confiar en otro segmento de red, si es que se debe hacer.

- Los segmentos de red deben ser diseñados en la confianza de las relaciones entre los usuarios y no en las necesidades de harware.
- Usar métodos de encriptación para asegurar la confidencialidad de la información.
- Monitorear la red, en busca de nuevos usuarios no autorizados.

Además de las reglas mencionadas, se puede proteger una red usando herramientas anti-sniffer, redes conmutadas y el uso de encriptación.

4.4.2.1 Herramientas anti-sniffer

Existen softwares que permiten a un administrador de red asegurar máquinas y servidores individualmente. Softwares para la detección de que NIC en modo promiscuo. Estas herramientas de detección deben ser usadas regularmente para la detectar a tiempo el uso de los Sniffer.

4.4.2.1.1 PromiScan

PromiScan (http://www.securityfriday.com/) es una utilidad de distribución gratuita diseñada para dar caza a los nodos promiscuos en una LAN rápidamente y sin crear una pesada carga en la red. Hay que tener en cuenta que localizar un nodo promiscuo es una tarea ardua, y que en muchos casos el resultado es incierto; no obstante, PromiScan consigue mostrar cada uno de esos nodos de una manera transparente, claramente visible. Para usar PromiScan es necesario contar con Windows 2000 Professional y haber instalado previamente el controlador WinPcap."

4.4.2.1.2 Detección en redes conmutadas

En redes conmutadas o que hagan uso de switches, la técnica de ARP poisoning o envenenamiento arp es la más efectiva. Esta técnica consiste, en modificar (envenenar) la tabla ARP de los host involucrados en el ataque para que éstos envíen a la red tramas Ethernet con destino la MAC del atacante. Esto significa que el switch entregará los datos de la comunicación a dicho host. Para evitar el refresco de la caché ARP es necesario el envió constante de arp-reply.

Una posible solución, o defensa, sería el uso de tablas MACs estáticas, con el fin de que no puedan ser modificadas, aunque en algunos sistemas Windows esto no es eficiente en un 100 por 100.

4.4.2.1.3 WinARP Watch v1.0

WinARP Watch v1.0 (http://www.securityfocus.com/data/tools/warpwatch.zip), no envía correo alguno a ningún administrador, pero mantiene puntualmente informado sobre la caché ARP, las correspondencias IP/MAC, cualquier nuevo par que se añada a la caché, etc.

La figura 4.2. presenta una alerta del programa.

Time	Action	IP Address	DNS Name	MAC Address
11:55:55	Added	192.168.4.1		00:04:76:97:B3:A9
11:55:55	Added	192.168.4.5		00:04:76:9A:66:A6
11:56:00	Added	192.168.4.15		00:01:02:E7:57:CF
11:56:00	Added	192.168.4.20		00:A0:24:4E:4E:4E
11:58:39	Added	192.168.4.8		00:10:4B:4D:15:BB
12:05:32	Ignored	192.168.1.0		00:00:00:00:00:00
12:05:40	Added	192.168.4.235		00:C0:85:27:39:15
12:45:59	Added	192.168.4.13		00:60:08:59:55:50
12:46:09	Added	192.168.4.10		00:A0:24:4E:51:6B
12:46:15	Added	192.168.4.16		00:60:08:96:D1:59
13:50:41	HAS CHANGED	192.168.4.8		00:04:76:F2:C9:5F
13:50:45	HAS CHANGED	192.168.4.5		00:04:76:F2:C9:5F
13:50:55	HAS CHANGED	192.168.4.5		00:04:76:9A:66:A6

Figura 4.2. Ventana WINRAP WATCH

Existe un tipo especial de switches que está preparado para que la tabla ARP no pueda ser modificada.

4.4.2.1.4 Ettercap

Ettercap **(** http://ettercap.sourceforge.net/) es capaz de escuchar redes basadas en hubs como en switches. Además puede escuchar conexiones SSH, incluso detectar otros envenenamientos o modificaciones de la tabla ARP.

4.4.2.2 Redes conmutadas (Switched Networks)

Una red conmutada es un buen obstáculo para un Sniffer. En un ambiente no conmutado, los paquetes son visibles por cada nodo de la red, en un ambiente conmutado, los paquetes son entregados a la dirección de destino. A diferencia de los HUBS, los conmutadores (switches) solo envían tramas al receptor designado, por lo tanto, una NIC en modo promiscuo en una red

conmutada no capturará todos los datos del tráfico local. Existen programas como *dsniff*, que permiten a un atacante monitorear una red conmutada.

4.4.2.3 Encriptación de datos

Esta es la mejor forma de protección contra la intercepción de tráfico. Es razonable asumir que en algún momento los datos pueden ser comprometidos, por ello la mejor defensa es asegurarse que el tráfico es imposible de leer, ilegible, por cualquier usuario, menos por el usuario receptor del trafico. No es difícil generar este tráfico, muchas organizaciones han desarrollado servicios SSL y TLS, y otros métodos que proveen mensajería segura, búsqueda en la red (web).

De esta forma un atacante puede ver en el tráfico el encabezamiento y el origen, pero no puede leer el contenido.

Al comparar el tráfico de una red sin encriptación en sus computadoras, el tráfico capturado se vería como muestra la figura 4.3.

```
21:06:30.786814 0:1:3:e5:46:6b 0:4:5a:d1:46:ad 0800 650: 192.168.1.3.32946 >
66.38.151.10.80: P [tcp sum ok] 1:585(584) ack 336 win 64080 <nop,nop,timestamp 608776
899338> (DF) (ttl 64, id 7468, len 636)
0x0000   4500 027c 1d2c 4000 4006 8074 c0a8 0103      E..|.,@.@..t....
0x0010   4226 970a 80b2 0050 54ac b070 78ef d6c3      B&.....PT..px...
0x0020   8018 fa50 c663 0000 0101 080a 0009 4a08      ...P.c........J.
0x0030   000d b90a 4745 5420 2f63 6f72 706f 7261      ....GET./corpora
0x0040   7465 2f69 6d61 6765 732f 6275 696c 642f      te/images/build/
0x0050   626c 6c74 5f72 645f 312e 6769 6620 4854      bllt_rd_1.gif.HT
0x0060   5450 2f31 2e31 0d0a 486f 7374 3a20 7777      TP/1.1..Host:.ww
0x0070   772e 7365 6375 7269 7479 666f 6375 732e      w.securityfocus.
0x0080   636f 6d0d 0a55 7365 722d 4167 656e 743a      com..User-Agent:
0x0090   204d 6f7a 696c 6c61 2f35 2e30 2028 5831      .Mozilla/5.0.(X1
0x00a0   313b 2055 3b20 4c69 6e75 7820 6936 3836      1;.U;.Linux.i686
```

Figura 4.3. Trafico no encriptado

Cuando el tráfico de una red es encriptado, él tráfico capturado se vería como se muestra en la figura 4.4.

Figura 4.4. Trafico encriptado

Además de las herramientas anti-sniffer, las redes conmutadas y el uso de redes encriptadas, existen pruebas para la detección de Sniffers en la red.

4.4.2.4 Técnicas de detección

4.4.2.4.1 Test DNS

En este método, la herramienta de detección en sí misma está en modo promiscuo. Se crea numerosas conexiones TCP falsas en él segmento de red, esperando un sniffer pobremente escrito, atrape estas conexiones y resuelva la dirección IP de los inexistentes hosts. Algunos sniffers realizan búsquedas inversas de DNS en los paquetes que capturan. Cuando se realiza una búsqueda inversa DNS, la utilidad de detección de un sniffers detecta la petición de las operaciones de búsqueda para ver si el objetivo es aquel que realiza la petición del host inexistente.

4.4.2.4.2 Test PING

Este método confía en un problema en el núcleo de la máquina receptora. Se puede construir una petición tipo "ICMP echo" con la dirección IP de la máquina sospechosa de hospedar un sniffer, pero con una dirección MAC deliberadamente errónea. Se envía un paquete "ICMP echo" al objetivo con la dirección IP correcta, pero con una dirección de hardware MAC de destino distinta. La mayoría de los sistemas desatenderán este paquete ya que su dirección MAC

es incorrecta. En algunos sistemas Linux, NetBSD y NT, puesto que el NIC está en modo promiscuo, el sniffer asirá este paquete de la red como paquete legítimo y responderá por consiguiente. Si el blanco en cuestión responde a la petición, se sabrá que está en modo promiscuo. Un atacante avanzado puede poner al día sus sniffers para filtrar tales paquetes para que parezca que el NIC no hubiera estado en modo promiscuo.

4.4.2.4.3 Test ICMP

Ping de Latencia. En éste método, se hace un ping al blanco y se anota el Round Trip Time (RTT, retardo de ida y vuelta o tiempo de latencia). Se crean centenares de falsas conexiones TCP en él segmento de red en un período de tiempo muy corto. Se espera que el sniffer esté procesando estos paquetes a razón de que el tiempo de latencia incremente. Entonces se hace ping otra vez, y se compara el RTT, esta vez con el de la primera vez. Después de una serie de tests y medias, se puede concluir o no si un sniffer está realmente funcionando en el objetivo o no.

4.4.2.4.4 Test ARP

Se envía una petición ARP al objetivo con toda la información, exceptuando por la dirección de hardware de destino que es errónea. Una máquina que no esté en modo promiscuo nunca verá este paquete, puesto que no era destinado a ellos, por lo tanto no contestará. Si una máquina está en modo promiscuo, la petición ARP sería considerada y el núcleo la procesaría y contestaría. Si la máquina contesta, se sabrá que esta en modo promiscuo.

4.4.2.4.5 Test ETHERPING

Se envía un "ping echo" al host a testear con una IP de destino correcta y dirección MAC falseada. Si el host responde, es que su interfaz está en modo promiscuo, es decir, existe un sniffer a la escucha y activo.

El uso de estos test pueden resultar difíciles de aplicar, por ello se pueden usar softwares, alguno de ellos mencionados en el punto 4.4.2.1, los cuales permiten la detección de Sniffers en la red.

4.5 SPYWARES [5][14][11]

Los Spywares tienen cierta similitud con los virus, pero a diferencia de estos, los spywares no tiene código dañino para los computadores, por lo tanto los Anti-Virus comunes no los pueden reconocer ni eliminar.

Los spywares son pequeños programas que se instalan en los sistema con la finalidad de robar datos y espiar los movimientos por la red. Luego envían esa información a empresas de publicidad de internet para comercializar con los datos recopilados.

Trabajan en modo 'background' (segundo plano) para que el usuario no se percate que están hasta que empiecen a aparecer los primeros síntomas.

4.5.1 Forma de entrada a los computadores

Estas son algunas de las formas de las cuales pueden ingresar a un computador:

- Al visitar sitios de Internet que nos descargan su código malicioso (ActiveX, JavaScripts o Cookies), sin nuestro consentimiento.
- Acompañando algún virus o llamado por un Troyano.
- Estando ocultos en un programa gratuitos (Freeware) los cuales al aceptar sus condiciones de uso se acepta que cumplan sus funciones de espías.

4.5.2 Información que recaban

Pueden tener acceso a:

- Correo electrónico y el password
- Dirección IP y DNS
- Teléfono
- País
- Paginas que se visitan y sus temas
- Tiempos de permanencia y frecuencia regreso
- Software instalados

- Compras haces por Internet y datos más importantes como número de la tarjeta de crédito y cuentas de banco.

4.5.3 Spywares más comunes

- AdSofware
- Alexa
- Cydoors
- Gator
- Web3000
- Webhancer
- CoolWebSearch
- BlazeFind.Bridge
- Xupiter, Hotbar
- Kazaa
- etc

4.5.4 5 principales síntomas de infección

1. Se cambian solas las página de inicio, error y búsqueda del navegador.
2. Se abren ventanas pop-ups, incluso sin estar conectados y sin tener el navegador abierto, siendo la mayoría de temas pornográficos.
3. Barras de búsquedas de sitios como la de Alexa, Hotbar, etc.. que no se pueden eliminar.
4. Botones que aparecen en la barras de herramientas del navegador y no se pueden eliminar.
5. La navegación por la red se hace cada día más lenta.

4.5.5 Herramientas necesarias para la eliminación

- Ad-Aware 1.04 SE Personal

  La nueva versión (Second Edition) de esta poderosa e indispensable herramienta totalmente gratuita, de fácil utilización, diseñada para eliminar todo tipo de Spywares/Awares, con total seguridad y garantía.

  Se actualiza casi semanalmente añadiendo remedio a cuanto nuevo Spyware es detectado.

http://www.infospyware.com/Anti-Spywares.htm

– SpywareBlaster 3.2

Una herramienta fundamental para la prevención de ataques de spywares. No los elimina; simplemente deshabilita los controles ActiveX de los más conocidos spywares. Lo recomienda Spybot para inmunizar el sistema.

http://www.infospyware.com/Anti-Spywares.htm

– HijackThis 1.98.2

Es una pequeña herramienta que permite detectar y, eventualmente, eliminar las modificaciones hechas por programas de terceros en el navegador Explorer. (Toolbars, Paginas de Inicio, Paginas de búsqueda, etc) Hay que tener mucho cuidado con los cambios en el Registro. Es recomendable hacer una copia de seguridad del Registro en caso de.

http://www.infospyware.com/Anti-Hijackers.htm

– CWShredder 1.59.1

Uno de los mejores eliminador de paginas de inicio spywares y de dialers, elimina el famoso "CoolWebSearch"

– Buster 3.0

Elimina los spywares "HomeSearch" y otros que nos cambian la página de inicio por "about :blank"

– EliStarA.exe

Detecta y elimina el parásito "StarPage.FH" y sus todas sus variantes los cuales se encargan de cambiar la página de inicio por una "Search For..."

http://www.zonavirus.com/descargas/EliStarA.exe

4.5.6 Pasos para la eliminación de spyware

1. Descargar las principales herramientas arriba mencionadas (Ad-Aware SE, Spybot S&D, SpywareBlaster, etc)
2. Actualizarlos y configurarlos. (Ad-Aware SE actualiza semanalmente)
3. Apagar el System Restore o "Restaurar Sistema del las propiedades de Mi PC (Solo en Win ME y XP).

4. Desconectar los cables de red y de Internet. (quedar totalmente desconectado de la red).
5. Es aconsejable iniciar Windows pulsando la tecla F8 y seleccionar entrar en modo a prueba de fallos.
6. Escaneada la computadora con Ad-Aware SE en modo completo y con Spybot S&D en modo residente en memoria y en sistema de inmunización.
7. Eliminar todo lo que encuentren, en caso de que algo no pueda ser eliminado anotar el nombre para buscarlo en el registro o usando el HijackThis.
8. Si la página de inicio en el IE fue cambiada, entrar en las propiedades y cambiarla a mano antes de conectar a Internet.
9. Eliminar las cookies, el historial y los archivos temporales de Internet a mano, antes de conectar a internet.
10. Reiniciar el PC
11. Volver a escáner la PC para comprobar de que este totalmente limpio.
12. Complementar el Spybot en su sistema de inmunización con el SpywareBlaster 3.1 para prevenir futuros ataques.
13. Instalar un cortafuegos como Outpost Firewall, Norton Security, Zone Alarm.
14. Si no encuentran nada conectar nuevamente Internet y mantener los programas siempre actualizados.

Si se navega mucho por Internet, se recomienda que se actualicen periódicamente los softwares, como Ad-Aware, además de escanear el sistema semanalmente.

CAPITULO V
AGUJEROS DE SEGURIDAD

5.1 Concepto de agujeros de seguridad [5][6]

Un agujero es cualquier falla de hardware o software que permite a usuarios no autorizados obtener acceso o incrementar su nivel de acceso sin previa autorización. Un agujero puede ser cualquier cosa, un ejemplo es la contraseña de la CMOS (bios) de los computadores personales que se pierde cuando la batería de la CMOS es cortocircuitada, desactivada o removida. Incluso la posibilidad de empezar una sección de usuario de modo individual en una estación de trabajo puede ser clasificada como un agujero. Esto ocurre así porque permitiría a un usuario malicioso comenzar a ingresar comandos que podrían apoderarse del control del computador.

Por lo tanto, un agujero es alguna forma de vulnerabilidad. Cada plataforma de sistema tiene agujeros, tanto en hardware como en software.

5.2 Escala de vulnerabilidad

Existen diferentes tipos de agujeros:

- Agujero que permiten la denegación de servicios.
- Agujeros que permiten a un usuario, con privilegios limitados, incrementarlos sin autorización.
- Agujeros que permiten a usuarios externos (en sistemas remotos) acceso no autorizado a la red.

Estos tipos de agujeros y ataques pueden ser evaluados de acuerdo al peligro que presentan para el servidor victima. Algunos representan un peligro significante, que pueden destruir el objetivo. Otros son menos serios, calificando solo como molestias. La figura 5.1 muestra un tipo de escala de vulnerabilidad, por la cual se puede medir el peligro de los diferentes tipos de agujeros.

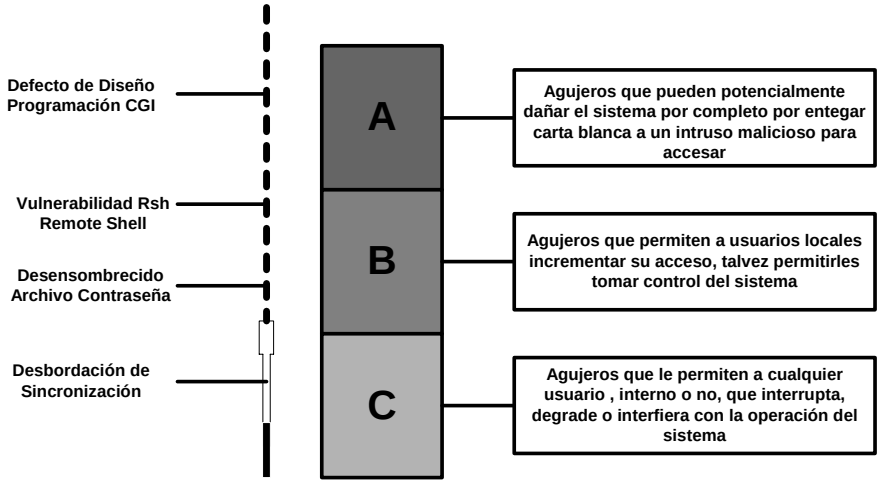


Figura 5.1. Escala de Vulnerabilidad

5.2.1 Agujero que permite denegación de servicios [5][6]

Los agujeros que permiten denegación de servicios, son calificados como C, y son los de mas baja prioridad. Este tipo de ataque son prácticamente basados en los sistemas operativos. Este tipo de agujeros son corregidos generalmente por los autores de los softwares o por parches del proveedor . la denegación de servicios son el tipo de ataques por el cual un individuo, o individuos, explotan aspectos de los paquetes de protocolo de Internet para denegar a otros usuarios el acceso legitimo a sistemas e información.

El ataque SYN TYP es aquel, en el cual se envían peticiones de conexión a un servidor en un gran volumen, causando que se atoche con cada petición. El resultado de esto es un servidor lento o inalcanzable.

5.2.2 Agujeros que permiten a usuarios locales acceso no autorizado

Manteniéndose alto en la escala jerárquica de agujeros, son el tipo de agujeros que permiten a usuarios locales obtener un incremento y un acceso no autorizado (clase B). Este tipo de agujeros son típicos de encontrar en aplicaciones en diferentes plataformas.

Un usuario local, es aquel que posee una cuenta en una determinada maquina o red. En el contexto, local se refiere a los privilegios de la cuenta de usuario, y no de la ubicación geográfica,

esto ya que se puede acceder por *telnet* a un sistema si es que se cuenta con los privilegios para ello, de esta forma el usuario puede estar alejado físicamente del sistema de red utilizado, pero dentro de ella lógicamente.

5.2.3 Agujeros que permiten a usuarios remotos acceso no autorizado (clase A)

Los agujeros clase A, son los mas temidos de todos y no es de sorprender que ocurren en sistemas pobre en administración o mal configurados. Los proveedores raramente prestan atención a aquellos agujeros que permiten a usuarios remotos desautorizados acceso.

Un ejemplo de una mala configuración, o de una falla en la configuración, es cualquier muestra de programa que permanece en el disco, aun cuando los documentos de la distribución notifique o aconseje que debe ser suprimido.

La mayoría de los servidores de web claramente contienen escasa documentación. Algunos archivos pueden existir, y aparentar ser tutóriales, sin embargo, como regla general, las distribuciones traen los siguientes elementos:

- Instrucciones de instalación
- Código ejecutable
- En algunos casos el código fuente
- Ejemplos de archivos de configuración, con comentarios combinados con códigos
- Ejemplos de programas CGI

Para crédito de aquellas distribuciones de softwares, muchos archivos de configuraciones ofrecen advertencias relacionadas con los ejemplos de programas. Sin embargo, no todo el mundo presta atención a aquellas advertencias. En ese caso, los programas pueden algunas veces, ofrecer permitir proveer a un intruso desde la nulidad de acceso a un acceso de root, o administrador principal o general.

5.2.4 Otros tipos de agujeros

Se encuentran agujeros en caso todo tipo de software de acceso remoto. Existe una gran lista de ellos, siendo alguno de ellos los que se listan a continuación:

- Ftp
- Gopher
- Telnet
- Sendmail
- Nfs
- Arp
- Portmap
- Finger

Estos programas, además de contener agujeros clase A, contienen agujeros clase B.

CAPITULO VI
ATAQUES REMOTOS

6.1 Ataques remotos [5]

Se define como cualquier ataque que es inicializado en contra de cualquier maquina remota (computadora) sobre la cual el atacante no tiene control. Una maquina (computadora) remota, es cualquier maquina que esta en red, que no es la propia, y que es alcanzada a través de algún protocolo a través de Internet o cualquier otra red o medio.

Es difícil que un atacante tenga contacto con la maquina (computadora) objetivo. El problema del atacante es determinar con quien se va a enfrentar y sus debilidades. El atacante puede obtener información de su objetivo sin que este se entere. Esto se logra si el la maquina objetivo no se utiliza algún tipo de protección. La mayoría de los usuarios de redes de Internet no utilizan ningún tipo de dispositivo de protección.

Un atacante buscara información que le entregue información para ingresar ha algún sistema, como el sistema operativo usado, claves de acceso de los sistemas con niveles de acceso (Linux, Windows NT, 2000, XP, Server).

Los sistemas operativos, como se menciono en capítulos anteriores, son diseñados y programados por equipos de personas, por lo tanto, no son infalibles, encontrándose errores de programación, tanto en el núcleo del sistema, como en las aplicaciones que corren en ella. Es en esa situación que el atacante hace uso de sus conocimientos en programación y de los errores de los sistemas y de sus aplicaciones, usando aplicaciones que buscan puertos abiertos.

Obteniendo los puertos en uso, el atacante comienza a probar diferentes formas para entrar a la maquina objetivo. Es común que el atacante encuentre el correo electrónico del usuario, o del administrador del sistema. Al poseer esa información, envía correos electrónicos con archivos adosados (attach), los cuales contienen códigos maliciosos (virus, exploits, troyanos, etc), que son utilizados para tomar control de la maquina objetivo, a través de los puertos encontrados.

Otra forma para tomar control de una maquina es usando portales de paginas web. Se logra a través de códigos maliciosos (scripts) introducidos al código fuente de una pagina web que es de interés para el usuario. Algunos ejemplos son los códigos usados en el lenguaje JAVA, los cuales pueden cargar pequeñas aplicaciones que se ejecutan en diferentes plataformas, ventajas del lenguaje JAVA. Otra forma, siguiendo la misma línea, es generando mensajes de petición para bajada (download) de alguna aplicación, necesaria para seguir con algún proceso relacionado a la ejecución dela pagina web. Ejemplos de esta situación son los portales donde se obtienen programas informáticos, números de serie de programas registrados, paginas con contenido pornográfico.

Generalmente, son introducidos pequeños códigos binarios, que son relacionados con el sistema de inicio (booteo) del sistema operativo comprometido. El uso de antivirus y firewall reducen este tipo de amenazas, pero no los evita.

Otra forma de ingresar a un sistema es compartiendo en la red archivos infectados con virus o troyanos, programas ejecutables de diferentes tipos, a través de programas de intercambio de archivos que usan diferentes tecnologías, como PEER to PEER. Algunos de los programas más conocidos son KAZZA, I-MESH, E-MULE. Además, estos programas contienen códigos que abren puertos en las computadoras que son utilizadas, generando nuevas entradas a los atacantes. Si el atacante es conocedor de los sistemas operativos, además de un buen programador, este podría entrar a un sistema operativo por algún puerto abierto, dejar y ejecutar alguna aplicación, como códigos ya mencionados, y de esa forma, tomar control completo del sistema. En el caso de servidores (host), el atacante investiga, además del sistema operativo, que aplicaciones se ejecutan en este, como web mail, servidores web, ftp, etc. Si el atacante no le interesa tomar control de la computadora para robar, dejar información, o utilizarla para generar nuevos ataques, cubriendo así sus pasos, puede generar ataques de DoS, generando grandes perdidas de información, las son traducidos a unidades económicas. Un claro ejemplo es la perdida de la ejecución de un portal para una empresa punto ***com***, cuyo negocio es la ventas de insumos. Al recibir este ataque, perderían clientes y oportunidades de ventas por estar fuera de servicio.

Otra forma de presentarse un ataque DoS, se produce cuando se produce la perdida de un servicio de otro tipo, excluyendo el ya mencionado, conectado a una red como lo es el servicio de impresión. Un ejemplo de este ataque es un ataque programado que se realizo al servicio de impresión de una escuela de graduados, anexo B. Este ataque tubo como génesis un escaneo a un segmento de red de la universidad, encontrando un IP con una identificación de una impresora HP. Se utilizo un programa de uso común, pero no se menciona por razones de seguridad. Al obtener el IP, más la información de ser una impresora en red, se procedió a investigar a quien pertenecía el IP asignado a esa impresora, esto al revisar los IP correlativos a este, encontrando información que identificaba a que edificio estaban asignados los IP de esa red. Se procedió a visitar el edificio y revisar algunas oficinas públicas, encontrando la impresora en la oficina de una secretaria. Se procedió en ese momento a tomar el modelo de la impresora mientras se hacían consultas a la secretaria de la escuela de graduados de esa facultad. Posteriormente, se obtuvieron los drivers de la impresora desde Internet y utilizando la red inalámbrica de la biblioteca central, la cual utilizaba una red asignada con IP dinámicos, sin identificación de usuario. Al ser instalados los drivers, se configuro el IP del servidor de impresión de la impresora HP, enviando a imprimir un documento de extensión .DOC en el cual se le advertía de la falla de seguridad del servidor de impresión, el cual podría ser atacado a través de una petición de impresión de varios documentos con miles de copias generando varias situaciones:

- Pérdida de la capacidad de enviar documentos que son los destinados a ese servidor de impresión.
- Agotar los insumos de impresión de la impresora.
- Obligar al administrador del servicio de impresión a apagar o desconectar de la red al servidor de impresión.

De esa forma se genero de forma sencilla un taque que hubiera generado perdidas económicas a una unidad de la Universidad Austral de Chile.

Otro tipo de ataque DoS, se obtiene con el conocido PING de la muerte, el cual genera una interrupción de la conexión de la red de la computadora de destino, llegando en muchos casos causando el reinicio o apagado instantáneo de la computadora.

Otro ataque que permite el control de algún sistema es a través de la ingeniería social, la que básicamente es convencer a un usuario a realizar algo que no debería, como el entregar información valiosa de un sistema con sus cuantas de accesos y contraseñas.

6.2 Niveles de ataque o sensibilidad [5]

En una red existen niveles de riesgo, ataque o de sensibilidad. Estos niveles están asociados a niveles de riesgos que se asocian a diferentes técnicas de ataque.

Los niveles de sensibilidad son muy similares en los distintos tipos de redes. Los riesgos más comunes son enumerados en una lista, la cual no cambia con el tiempo, suscitándose estos cuando se introduce (se crea) alguna nueva tecnología, como Active X, que permite la ejecución arbitraria de programas en la red.

6.2.1 Nivel 1

Los ataques clasificados en este nivel son prácticamente irrelevantes. Incluye ataques de denegación de servicios como bombardeos de e-mail, los cuales pueden ser solucionados rápidamente. La intención de estos ataques es la de generar una molestia, sin el sub valorizar el ataque de denegación de servicio (DoS) el cual puede resultar muy serio.

Ataques que fuerzan a maquina (pc) a reiniciarse (reboot), por sobre utilización del procesador, son considerados en este nivel, debido a que son problemas temporales.

Siendo que un ataque de denegación de servicio puede ser considerado de un nivel bajo de riesgo, también es considerado de un alto nivel de posibilidades.

Para generar ataques para este nivel no se requiere de grandes conocimientos ni experiencia.

Los DoS son tan comunes como los bombardeos de e-mail. Este ataque consiste en enviar reiteradamente mensajes, e-mail, a una victima o servidor especifico. Los mensajes contenidos en estos e-mails son de gran tamaño y con datos maliciosos, esto para consumir recursos adicionales de la red y el sistema. Si este ataque fuera DoS del sistema de correo electrónico.

6.2.2 Niveles 2 y 3

Estos niveles involucran que un usuario local adquiera acceso y permisos de lectura y escritura sobre archivos o carpetas en los cuales no tiene.

En caso de que un usuario local pueda tener acceso a carpetas y archivos importantes podría ser crítico, permitiendo llegar al nivel 3. Este es un asunto prioritario para los administradores de sistemas UNIX, LINUX, NT y versiones posteriores del sistema operativo Windows como Windows 2000 y XP.

Las amenazas de un usuario local se asocian directamente al tipo de red en que se encuentra. En una red privada o pública, cualquier usuario conectado a esta red seria catalogado como un usuario local llegando a ser un posible atacante. Generalmente un usuario local que se identifique como atacante, puede generar ataques con diferentes niveles de sofisticación, pero sin importar el nivel de habilidad, regularmente los ataques son vía TELNET.

6.2.3 Nivel 4

Esta relacionado con archivos internos accesados por un intruso. Este acceso puede variar. Podría hacer más que verificar la existencia de un archivo, podría leerlo o modificarlo. Este nivel incluye aquellas vulnerabilidades por las cuales usuarios remotos, sin cuentas validadas, pueden ejecutar un numero limitado de comandos en un servidor.

El mayor porcentaje de aquellos agujeros de seguridad se originan por una deficiente configuración de los servidores, deficientes CGI, y problemas de desbordamiento.

6.2.4 Niveles 5y 6

Estos niveles consisten en condiciones por las cuales situaciones pueden ocurrir y que nunca debería ocurrir. Cualquier agujero en estos niveles es fatal. En esta etapa usuarios remotos pueden leer, escribir y ejecutar archivos, lográndolo por medio de una combinación de técnicas.

Si se han evitado ataques en niveles inferiores, es difícil, llegar estar expuesto en este nivel de ataque. Podría generarse a este nivel un ataque por el uso de algún software defectuoso, o por

alguno que genere agujeros de seguridad a este nivel. Algunos programas de tipo PEER to PEER, o de administración pueden generarlos.

6.3 Respuestas a ataques por niveles [5]

Si descubren que se esta siendo atacado, la respuesta depende de la situación.

6.3.1 Respuesta ataques de primer nivel

Ya se ha descrito algunas formas de respuesta, pero una forma de prevenir más ataques es el filtrar, excluir las direcciones IP de donde se originan los ataques y contactar al proveedor de un servicio a Internet del atacante.

Existen inconveniencias menores con estos ataques, solo cuando un ataque DoS surge y esta relacionado con alguna otra forma de ataque, o si continua por algún tiempo, se deberá hacer más que excluir el trafico entrante. Si los ataques persisten, es recomendable contactar alguna autoridad relacionada con la seguridad informática.

6.3.2 Respuesta a ataques de segundo nivel

Estos ataques también pueden tratarse localmente. Básicamente, se puede congelar o eliminar la cuenta de un usuario local. Si este usuario hace un reclamo por la eliminación de su cuenta, hay que tener presente que aunque se le aconseje o advierta, con seguridad este volverá a las mismas costumbres. Es aconsejable no dar aviso de que la cuenta ha sido congelada o eliminada. Si se congela, se puede preservar la evidencia necesaria para probar el mal uso de esta, de no hacerlo, el usuario podría borrar todo rastro.

6.3.3 Respuesta a ataques de terceros, cuarto, quinto y sexto nivel

Si se experimenta ataques de niveles superiores al segundo, se esta en problemas, por lo cual hay que tomar varias acciones:

- Aislar el segmento de red para que la actividad ocurra en un área reducida.
- Permitir que la actividad continué
- Registrar todas las actividades exhaustivamente

- Identificar la fuente o las fuentes, de los ataques.

En este punto, se hace frente a un delincuente. Este nivel de ataques es considerado es considerado un crimen, y es penalizado por la ley.

6.4 Ataques bombardeos de e-mail y Spamming [5][6]

El Bombardeo de e-mail es caracterizado por un infractor (violador) que envía reiteradamente mensajes de e-mail a una dirección particular de e-mail.

E-mail Spamming es una variante del bombardero de e-mail, y se define por el envió de e-mail a cientos o miles de usuarios. Este ataque puede ser peor si se le responde el e-mail recibido.

El bombardeo de e-mail y Spamming puede contener una dirección de origen valida, la cual no es la de origen real, sino que se ha duplicado para ocultar el origen real.
A esta técnica se le conoce e-mail Spoofing. El e-mail Spamming, es casi imposible de prevenir debido a que cualquier usuario con una cuenta valida en Internet puede enviar múltiples correos a otra dirección valida de e-mail. Si es una gran cantidad de e-mail los que son dirigidos a, o a través de un sitio, el sitio puede sufrir una denegación de servicio (DoS), perdiendo la conectividad a la red, o fallando el sistema debiendo a:

- Sobrecarga de las conexiones de red.
- Uso de todos los recursos disponibles de la real.
- Llenando del disco de almacenamiento de datos como resultado de múltiples colocaciones de e-mail.
-

6.4.1 Detección y reacción al bombardeo de e-mail y Spamming

La lentitud repentina del sistema puede ser el resultado de que el agente de correo electrónico este tratando de procesar una gran cantidad de mensajes.

La reacción a esto es:

- Identificar el origen de estos y configurar los routers para prevenir la entrada de paquetes de ese origen.
- Contactarse con el origen para alertar de la actividad maliciosa.
- Mantener Actualizado las versiones de los programas y dominios encargados del reparto de e-mail, y aumentar las capacidades de registro para detectar o alertar en caso de este tipo de actividad.

6.4.2 Prevención

Hasta la fecha no hay forma segura de prevenir el bombardeo y Spamming de e-mail, y es imposible predecir el origen del próximo ataque.

Una forma de prevenir que lleguen mail al servidor de correo, es validar ante un firewall a los usuarios validos del servicio, evitando que se sobrecargue el servidor de correo con mensajes (e-mail) dirigidos al dominio pero a direcciones no validadas.

6.5 Ataque Spoofing [5][6]

La manipulación de los paquetes IP es muy peligrosa. El Paquete IP, además de su propio contenido, contiene una cantidad de información necesaria para transmitir datos desde la fuente al destino. El Spoofing consiste en la manipulación de estos datos y de la información necesaria para su transmisión. Esto consigue que la maquina (PC) receptor (destino) identifique a la fuente, atacante, como una maquina de su red, o como un servicio valido y seguro. Esta situación puede neutralizar las funciones de protección de los firewall.

El atacante al crear este contexto engañoso, engaña al destinatario del ataque, de forma que la victima tome una decisión que comprometa la seguridad de su equipo o que entregue información sensible, como claves y números de tarjetas de crédito.

Este tipo de ataque no solo se relaciona entre dos maquinas, ya que en el mundo real también ocurren estos ataques en cajeros automáticos falsos, los cuales capturan claves y tarjetas bancarias. Lo mismo ocurre con sistemas de pago con tarjetas de crédito.

Este tipo de ataque esta destinado a una maquina en particular generalmente, ya que es de gran dificultad la gestión del ataque.

6.5.1 DNS Spoofing

Consiste en el falseamiento de un IP ante la consulta de la resolución de nombre o viceversa. Se consigue mediante la manipulación de paquetes UDP pudiéndose comprometer el servidor de nombres de dominio (DNS) de algunos sistemas como Windows NT. Si se comprometiera un servidor, este puede afectar el cache de otro servidor de nombre de dominio (DNS Poisoning).

También se puede enviar datos falseados como respuesta a una petición real a una victima (esto sin usar un DNS real).

6.5.2 IP Spoofing

Consiste en generar paquetes IP con una dirección falsa en el campo FROM, y que es aceptado por el destinatario del paquete IP. De esta forma se oculta la identidad del atacante, sobre todo cuando se trata de ejecutar un ataque de denegación de servicios (DoS), de esta forma el destinatario de este ataque, ve que el ataque proviene de una red que no es de la red de donde se encuentra el atacante. Este tipo de ataque se hizo famoso al ser usado por Kevin Mitnich, uno de los más grandes hacker de Estados Unidos.

6.5.3 ARP Spoofing

La sigla ARP corresponde al protocolo de resolución de direcciones, el cual se utiliza para asignar direcciones IP a una dirección MAC.

Para entender la forma de APP Spoofing hay que entender el funcionamiento ARP.

El paquete IP antes de ser enviado por el emisor, este debe conocer la dirección MAC que tiene asignado el IP al cual va dirigido el paquete IP. Para obtenerlo, la máquina emisora, el sistema operativo, genera una petición ARP. La petición ARP es el equivalente a preguntar si la dirección IP es X.X.X.X., y si la respuesta es positiva, entonces se le es enviada la dirección MAC de regreso. Esta petición es transmitida por broadcast a todas las maquinas de la red. Los sistemas operativos poseen un cache de respuestas ARP, para minimizar la congestión en la red

causada por estas peticiones, por ello, cada vez que se recibe una respuesta ARP, actualiza su cache con la nueva tabla IP/MAC.

Comprendiendo lo anterior, el ARP Spoofing consiste en reconstruir estas respuestas ARP, enviándolas a la maquina que se desea atacar, engañándola y haciéndola creer que una maquina B es la maquina A. De tener éxito, la maquina atacada no podía distinguir el engaño, y mucho menor saber el origen del ataque. Esto también se conoce como ARP Poisoning y se asemeja al DNS Poinsoning.

6.5.4 Web Spoofing

Este ataque es uno de los más comunes de encontrar, relacionado con los ataques Spoofing. Su finalidad es engañar a la victima, haciendo creer que una pagina web imitada a la real. El atacante crea una pequeña web idéntica a la original, pero albergada en otro servidor. Incluso las conexiones seguras SSL pueden ser duplicadas. Para lograrlo desarrolla un código por el cual crea una ventana del navegador correspondiente, de inofensiva apariencia. A partir de ahí, enruta todas las páginas dirigidas al equipo atacado, consiguiendo así, poder engañar a la victima, logrando sus intenciones.

De esta forma el a creado una página web falsa que es controlada por el atacante. Uno de los riesgos seria si se duplicara la página electrónica de un baneo, en la cual se le ingresa la identificación y la contraseña de un cliente, el atacante el apoderaría de dicha información logrando robar dinero de aquella cuenta. También podía ocurrir con web-mail. Existen formas para prevenir, o al menor identificar el ataque[16].

CAPITULO VII
FIREWALL

7.1 ¿Que es Firewall? [1][2][5][6][15]

Un firewall es un dispositivo usado para prevenir que un extraño obtenga acceso a la red protegida por este. Es una combinación de hardware y software. Comúnmente estos implementan reglas y esquemas de exclusión de direcciones o protocolos que usan las aplicaciones. Un firewall puede estar compuesto por software, hardware o por ambos. Cuando se trata de un firewall de software (Ej: Zone Alarm), pueden encontrarse algunos del tipo propietario o gratuito.

El hardware puede ser cualquiera que soporte el software que se esta utilizando. También pueden ser utilizados router como firewall. Los routers poseen características avanzadas de seguridad, incluyendo la capacidad de filtrar direcciones IP. El proceso de filtrado de dirección IP permite definir que direcciones IP son permitidas. Algunos tipos de routers tienen la capacidad de filtrar paquetes con lo cual aumenta la capacidad de protección gracias a las capacidades de los router, se utilizar interconectadas según lo muestra la Figura 7.1.

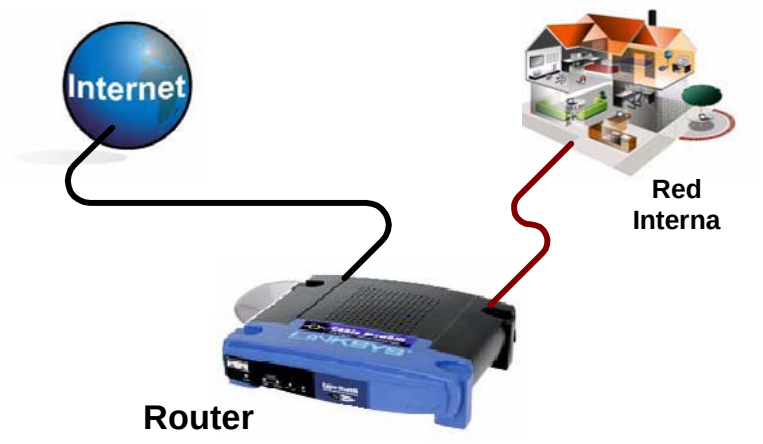


Figura 7.1. Router

7.2 Tipos de Firewall [1][2][5] [6]

Existen diferentes tipos de firewall, y cada uno tiene ventajas y desventajas. Los más comunes son los firewall a nivel de red. Estos son basados en routers. Las reglas de quien y que puede ser accesazo a la red es aplicado al nivel de ruteo. Este esquema es aplicado por una técnica llamada ***filtraje de paquetes***, lo cual consiste en un proceso en el cual se examina los paquetes que arriban a un router procedente de una red externa.

En la configuración de un firewall, basado en un router, la dirección de origen de cada conexión entrante es examinada. Después de que cada conexión IP de origen ha sido identificada, sin importar las reglas que la configuración haya emitido será forzado a seguir o a detenerse. Por ejemplo, si la configuración indica que ningún trafico de red sea aceptado en la red de la Universidad Adolfo Ibáñez (UAI), el router rechazara cualquier paquete que provenga de uia.com. Este tipo de router configurado como firewall es rápido, ya que chequea la dirección de origen por lo que no hay una demanda real en el router.

Este tipo de configuración tiene la debilidad que solamente filtra las direcciones IP que son parte de la lista que posee el router.

Se puede emplear la técnica de filtraje de paquetes con el firewall basado en router, disminuyendo su debilidad de filtrado de direcciones IP.

El encabezado de la dirección IP no es el único encabezado que el router puede identificar, también puede identificar otros campos. La tecnología de filtrado de paquetes se a sofistificado, se pueden aplicar reglas relacionadas a la información de los paquetes, usando índices para tiempos, protocolos, puertos, entre otros parámetros.

Aun con todas estas técnicas de filtraje, pueden generarse ataques a través de este tipo de firewall, ya que existen aplicaciones que usan puertos de forma dinámica, es decir, cambian el puerto, así es que si se tiene designado por defecto uno, puede realizar su conexión a Internet. En este caso la lista que tiene declarada el firewall no es de gran ayuda.

Para evitar este tipo de problema es recomendable configurar el router o firewall, cerrado todos los puertos tanto en el modo UDP como TCP, y solo abrir los puertos que se requieran, como el 80 para navegar en Internet y el SMTP, POP para la recepción y envío de e-mail.

7.3 Firewall de nivel de aplicación [2][6]

Esta programado para comprender el trafico en el nivel de aplicación de usuario (capa 7 del modelo OSI). Provee de accesos al nivel de usuarios al nivel de protocolo de aplicaciones. La habilidad de registrar y controlar todo el tráfico de entrada y salida es una de las principales ventajas de poseer una puerta de enlace a nivel de aplicación.
Para que cada aplicación sea transmitida, la puerta de nivel de aplicación, utiliza un código de propósito especial. Gracias a este código, la puerta de aplicación provee un alto nivel de seguridad.

La desventaja de este tipo de firewall, es que debe existir un código por cada aplicación que se utiliza, pero a la vez es una ventaja ya que ninguna aplicación puede pasar a través del firewall a menos que la puerta a nivel de aplicación provea la autorización.

Programas que reúnen este tipo de características son:

- Aladin E-Safe Personal Firewall
- McAfee Firewall
- Norton Personal Firewall
- Sygate Personal Firewall
- Tiny Personal Firewall
- Zone Alarm

Zone Alarma, es el firewall que más ventajas a demostrado tener. No Utiliza una gran cantidad de recursos de la maquina, además de su fácil administración. Una de las cualidades más sobre saliente es que la empresa lo a puesto para uso gratuito para el uso personal.

Posee una interfase grafica de fácil entendimiento y manejo, permitiendo a un inexperto su configuración. Posee un sistema que permite establecer los niveles de seguridad. Se pueden añadir servidores o rangos de direcciones IP a su lista de sitios de confianza.

Cuando algún programa intenta conectarse, enviar información fuera del sistema, Zone Alarm genera una alarma automática, preguntando que debe hacer, la respuesta a esta pregunta genera reglas que son almacenadas en una lista, que posteriormente puede ser modificada. Este sistema es más lento que un sistema de firewall basado en un router, ya que utiliza recursos propios de la maquina en la cual esta instalado.

La desventaja es que solo protege a la maquina que lo tiene instalado.

7.4 Seguridad para sistemas inalámbricos [2][6][12]

Stateful Packet Inspection (SPI) inspecciona los paquetes de entrada para asegurar que corresponden a una petición de salida. Datos que no han sido pedidos son rechazados. Los datos de entrada son chequeados en una lista de petición de salida para confirmar que concuerde con una solicitud realizada. El ataque de un hacker es bloqueado debido a qué no concuerda con el criterio de lo que ha sido solicitado.

Con las tecnologías NAT y SPI, es posible proteger una red de los ataques en Internet, dificultándole la entrada de hacker a los sistemas. Sin embargo, en la actualidad existen redes inalámbricas, por lo que es importante conocer las nuevas amenazas de seguridad para estas redes inalámbricas.

Debido a que las redes inalámbricas envían señales, a través del aire para comunicarse, es posible que otros sintonicen estas señales. Un hacker podría, de esa forma, identificar la señal, logrando no solamente entrar en la red local, sino que acceder al servicio de Internet sin pagar por ella.

Las redes inalámbricas son muy convenientes y fáciles para conectar dispositivos. Sin embargo, por transmitir información a través del aire, la red se vuelve vulnerable a la

interceptación y de los ataques, debido a que un hacker no necesita una conexión física a una maquina o a los dispositivos de la red.

Un hacker podría encontrarse en una casa o edificio cercano, o un auto estacionado en las proximidades como lo indica la figura7.2.

Figura 7.2 Proximidad de un Hacker

Para proteger la información inalámbrica, se deben emplear métodos adicionales de seguridad inalámbrica Estos métodos son simples para que se puedan realizar en la configuración inicial de un router, pero existen otros niveles avanzados de seguridad como WEP (Wired Equivalency Protocol), WPA (WI-FI Protected Access) Y MAC (Media Access control) Address Filtering.

Al igual que en las redes físicas, todas las redes inalámbricas poseen un nombre que las identifica. En las redes inalámbricas es conocido como Service Set Identifier (SSID). Quien desee conectarse a una de estas redes, debe conocer el nombre de la red a la cual se desea conectar.

Por defecto, todo los ruter y puntos de acceso inalámbricos, publican su nombre para facilitar a los usuarios la conexión a ellas. Cuando se desactiva la publicación del SSID, la red ya no anuncia el su existencia, por lo cual, si alguien quisiera conectarse, deberá conocer el SSID.

7.4.1. MAC Address Filtering

Ya es sabido que MAC (Media Access Control) Address es una identificación única que posee cada dispositivo de red. El filtrado de dirección MAC (física) consiste en identificar que dispositivos están permitidos para acceder la red inalámbrica.

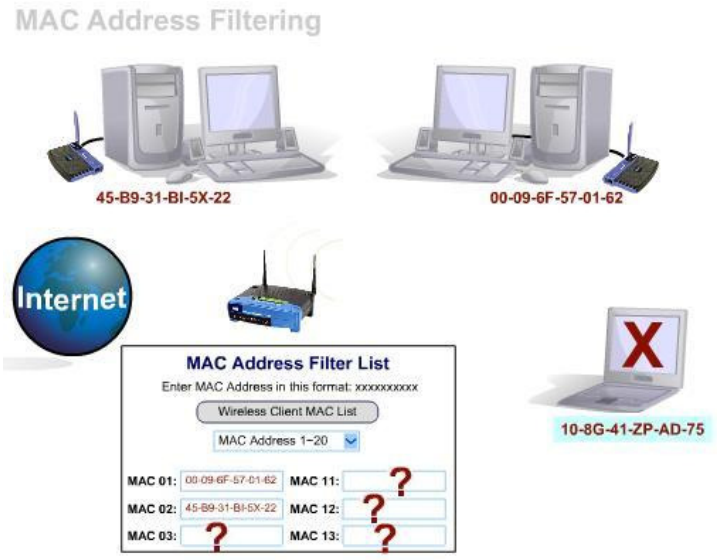


Figura 7.3 MAC Address Filtering

Solamente los dispositivos cuyas direcciones MAC han sido registradas en la base de datos (lista) del router, podrán acceder a la red inalámbrica, de lo contrario no podrán acceder a esta red como lo muestra la figura 7.3.

7.4.2. Wired Equivalency Protocol (WEP)

Es una característica que en encripta el tráfico de red a través del aire. WEP codifica la información usando una llave de codificación, enviada con anterioridad por el aire. Cada unidad que la recibe, deberá poseer la misma llave para decodificar la información. Las llaves pueden

generarse de 64 bit o 128 bit de tamaño. Cuantos más bits posea la llave de codificación, mayor deberá ser la codificación.

La llave que se use para WEP, debe ser utilizada para todas las configuraciones de los dispositivos de la red. Si no se utiliza esta llave en algún dispositivo, este no podrá decodificar la transmisión inalámbrica.

Este método es considerado un método básico de encriptación. A pesar que es un sistema confiable, puede ser traspasado por equipos de alta tecnología. Un hacker puede encontrar esta llave codificación y podría ingresar a la red.

Existen softwares que son usados por atacantes para capturar datos enviados entre los dispositivos inalámbricos, para descubrir la llave WEP, figura 4.

Figura 7.4. WEP

Una forma de evitar esta situación es cambiando periódicamente la llave WEP, de esta forma el atacante deberá repetir el procedimiento por descubrir la nueva llave.

7.4.3. WI-FI Protected Access (WPA)

La llave WEP es estática, es decir, no cambia en el tiempo por lo que se puede descubrir con el tiempo.

Para evitar esta situación se implementa una solución donde se genera una llave dinámica, que constantemente va combinando. A esta solución el le conoce por WPA.

WPA ofrece llaves para codificación de un tamaño de 256 bit, lo que genera una dificultad exponencial para un atacante al momento de tratar de decodificarla, ya que también es dinámica. Si se lograra decodificar, para ese momento el sistema ya tendría una llave nueva.

Figura 7.5. WPA

7.5. Red Virtual Privada (VPN) [1][2][4][5][6][7]][8][12]

Existen muchos beneficios al momento de implementar y poseer una red, pero muchas de estas requieren que el usuario deba permanecer en la proximidad de esta para que de forma segura y sencilla pueda obtener acceso a esta. Además se han popularizado los sistemas portátiles como notebook y agendas electrónicas personales tanto para el hogar como para los negocios, por ello, más usuarios han tenido la necesidad de acceder a sus redes remotamente. Internet provee una gran vía para que los usuarios se conecten a sus redes.

VPN, Red Virtual Privada (Virtual Prívate Networking), es una tecnología de seguridad que permite a un usuario acceder a una red remota desde un computador que se encuentra en otra red, figura 7.6.

Figura 7.6. VPN Simple

El usuario puede acceder a la red de un hogar o de su oficina, a través de Internet usando la tecnología de codificación VPN, la cual básicamente oculta un tráfico de cualquiera en Internet.

Formando un túnel VPN, figura 7.7, el trafico viaja desde y hacia la red que esta oculta, por lo que no puede ser vista, por ende, saboteada por nadie en la red.

Figura 7.7. VPN Codificada

La tecnología VPN permite seguridad a los e-mails y al compartir archivos tal como si se estuviera trabajando frente a una maquina de la red que se accesa.

Para crear un túnel VPN, deben existir dispositivos VPN en cada punto de la conexión. Los dispositivos VPN incluyen router VPN, adaptadores VPN, softwares VPN, figura 7.8.

Si una oficina posee un router VPN a la entrada de la red, el usuario remoto se conectara de manera segura por medio de otro router VPN al router VPN de la oficina, también se lograría usando un adaptado VPN conectado a la computadora, o instalarlo en software VPN.

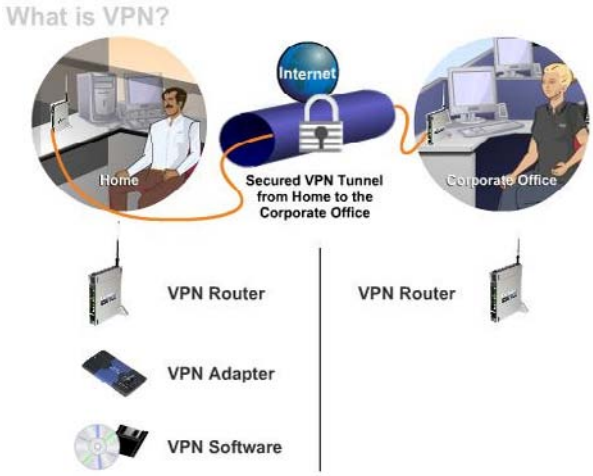


Figura 7.8. Periféricos VPN

7.6 Comparación seguridad entre sistemas cableados e inalámbricos [12]

Después de haber conocido los sistemas de seguridad de los sistemas cableados e inalámbricos se puede llegar a comparar ambos sistemas. La figura 7.9 la comparación del sistema de seguridad cableado, y el sistema inalámbrico, el que además posee otras características debido a que se transmite por el medio aéreo. Como se aprecia en la figura 7.9, se le ha añadido filtraje de dirección MAC, WEP Y WPA. Por esto, se puede concluir que los sistemas inalámbricos poseen una mayor seguridad en especial al momento de usar las llaves de codificación tanto en WEP y WPA. En el sistema de cableado, el trafico no es codificado, por lo que con un sistema Snifer se puede obtener información del trafico que por el sistema inalámbrico no se podría.

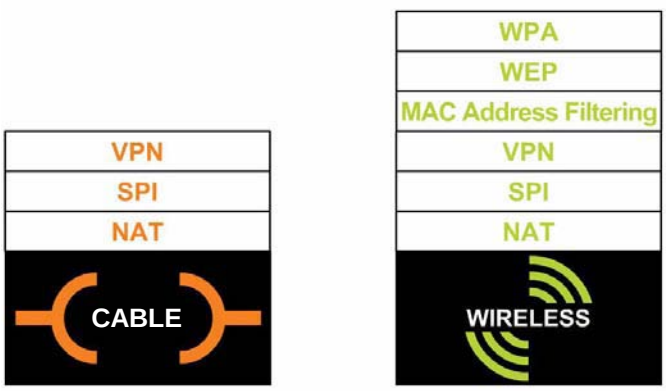


Figura 7.9 Comparación Tecnologías

CAPITULO VIII
DISEÑO DE POLÍTICA DE SEGURIDAD PARA UNA RED

Una política es un protocolo documentado que describe el sistema de seguridad concerniente a una red de una organización. Este documento describe los pasos a seguir para generar un sistema seguro y estable, que permita tanto a usuarios como al sistema en si, mantener sus bienes de información seguro de cualquier tipo de ataque intencional como casual.

El gestor de una política de seguridad contempla reglas orientadas a la identificación de recursos, amenazas, responsabilidades de los usuarios en la red, planes de acción cuando la política de seguridad es violada. Además entrega procedimientos de administración de la red.

Hay que considerar que una organización puede tener una red compuesta de múltiples subredes y fuentes de información, siendo controladas estas subredes por diferentes administradores, los cuales pueden tener diferentes metas y objetivos para las redes que administran. Si estas redes no están interconectadas, cada administrador puede tener sus propias políticas de seguridad. Si son parte de una red central, estos administradores deben de seguir las políticas centrales de seguridad, las cuales no irán en contra de políticas internas que los administradores, de las subredes, implementen para aumentar la seguridad de estas. Lo importante es mantener metas comunes de seguridad.

Las metas deben contemplar la seguridad de todos los elementos y recursos que forman la red y las subredes como:

- Estaciones de trabajo
- Servidores
- Dispositivos de interconexión: Router, Hubs, Switches. etc.
- Terminales de servidores.
- Software de aplicaciones y de sistemas de redes.
- Cable de redes.
- Información en archivos y bases de datos.

La política de seguridad debe de tomar en cuenta la protección de estos elementos.

Debido a que una red puede estar conectada a otras redes (ej: redes bibliotecarias), la política de seguridad debe considerar la necesidades y requerimientos de todas las redes interconectada.

Este es un punto importante a considerar, ya que al proteger los intereses de la red que se administra se puede perjudicar a otras redes.

8.1 Metodología de generación de la política de seguridad [2][4][5][6]

Definir una política de seguridad de una red significa desarrollar procedimientos y planes que resguarden los recursos de la red en contra de la pérdida y daño de esta. La metodología para desarrollarla es examinando las siguientes preguntas:

- ¿Qué recursos son los que se tratan de proteger?
- ¿De quiénes se deben proteger
- ¿Cuáles son las probables amenazas?
- ¿Cuan importante es el recurso a proteger?
- ¿Qué medidas se pueden ejecutar para proteger los bienes de forma efectiva?
- Examinar periódicamente la red para observar si deben cambiar los objetivos de trabajo de la política de seguridad

La tabla 8.1 muestra la tabla que es usada para desarrollar la metodología para preparar una política de seguridad

Recursos de Red			Tipos de Usuarios a Protegerse	Probabilidad de Ataque	Medidas a Implementar para Proteger los Recursos de Red
Número	Nombre	Importancia del Recurso			

Tabla 8.1 Desarrollo metodología para política de seguridad

- La columna número de recurso de red es el número de identificación interno de la red de los recursos que se protegerán (si es aplicable).
- La columna nombre de recurso de red es el nombre que describe el recurso.
- La columna importancia del recurso, puede ser expresado en una escala numérica del 0 al 10, o en expresiones como bajo, medio, alto, muy alto etc.
- La columna tipo de usuario a protegerse lleva las designaciones como interno, externo, invitado, nombre de grupos como asistentes de corporación, usuarios de contabilidad, etc.
- La columna de probabilidad de ataque usa las mismas escala que la columna de "Importancia de recurso de red"
- La Columna medidas a implementar para proteger los recursos de red tienen valores como "permisos de operación de sistema" para archivar y directorios, "seguimiento de alerta", para servicios de red, "Firewall" y "enmascaramiento por router" para servidores y dispositivos de red, o cualquier descripción de tipos de control de seguridad.

Se debe considerar que el costo de implementación de seguridad debe ser menor al costo que tiene el recobrar los bienes afectados ante un ataque de seguridad. Puede llegar a ser difícil la implementación de una política de seguridad si no cuentan con los conocimientos necesarios sobre lo que se desea proteger y de los orígenes de amenazas. Para lograrlo se deberá pedir ayuda a otros que tengan mayor conocimiento para lograrlos.

8.2 Asegurar las responsabilidades de la política de seguridad [2][5][6]

Un aspecto importante en la política de seguridad de una red es asegurar que cada involucrado conozca su responsabilidad para el mantenimiento de la seguridad. Es difícil que una política de seguridad anticipe todas las posibles amenazas.

Deben existir varios niveles de responsabilidad asociados con la política de seguridad. Cada usuario de la red debe ser responsable de resguardar su contraseña. Un usuario que facilite su cuenta aumentada la posibilidad de comprometer otras cuentas, así como recursos. Por otro lado, los administradores de redes y de sistemas de administración son responsables de mantener toda la seguridad de la red .

La organización debe facilitar los instrumentos necesarios para comprometer y obligar a los usuarios y administradores a mantener las políticas de seguridad.
Firmar documentos, contratos o compromisos donde se estipulan compromisos y sanciones a los infractores, son herramientas que permiten el correcto uso de los recursos, permitiendo disminuir los riesgos que un usuario podría generar.

La prohibición del uso de equipos para uso personal, no descargar información que no sea relacionada a la organización, la no utilización de software no autorizados por la organización, son algunas reglas que son parte de una política de seguridad.

Al crear la responsabilidad en la política de seguridad, hay que tener en cuenta que cada red o subred tiene reglas o políticas distintas. Esto se genera al desarrollar un estudio de análisis de riesgo, capitulo 3.5.1.4.

Este análisis entrega la información que indica la o las redes con mayor riesgo e importancia, por lo que la responsabilidad de un usuario que utiliza estas redes es mucho mayor a uno que utiliza una red de mejor importancia para la organización.

8.3 Responsabilidades y uso de la red [2]

Existe un número de asuntos que deben ser cubiertos cuando se desarrolla una política de seguridad:

- ¿Quién tiene permitido el uso de los recursos?
- ¿Cuál es el uso apropiado del recurso?
- ¿Quién esta autorizado para conceder acceso y aprobar el uso?
- ¿Quién tendrá privilegios de administrador?
- ¿Cuáles son los derechos y responsabilidades de los usuarios?
- ¿Cuáles son los derechos y responsabilidades del administrador de sistemas versus aquellas de un usuario?
- ¿Qué se debe hacer con información sensible?

8.3.1 Identificando quien debe ser autorizado para el uso de los recursos de red

Se debe elaborar una lista de usuarios que necesiten acceder a los recursos de la red. Los usuarios pueden ser parte de grupos de cuentas como usuarios abogados, ingenieros, administradores, etc. Se debe incluir una clase de usuarios, llamados usuarios externos, los cuales acceden a la red de otro lugar, siendo estos miembros de la empresa, accediendo remotamente.

8.3.2 Identificación del uso apropiado de un recurso

Después de identificar a los usuarios que accesarán los recursos de la red, se debe proveer los lineamientos para un uso responsable de ese recurso. Estos lineamientos dependerán de la clase de usuario, como desarrolladores de software, estudiantes, facultativos, usuarios externos, etc.

Para cada tipo de usuario existirá una lineamiento distinto. La política deberá declarar que tipo de uso de la red es aceptable, y que tipo de uso es restringido. La política que se desarrolla es llamada “Política de uso aceptable” (PVA) para la red. Si el acceso a recursos de la red es restringido, se debe considerar el nivel de acceso de las distintas clases de usuarios que se tienen.

La PVA debe ser clara que al irrumpir en una cuenta o eludir la seguridad, no está permitido, de esa forma se evitan problemas legales por parte de los miembros de la organización que hayan

eludido la seguridad de la red ya que ellos pueden acusar de que no fueron informados apropiadamente o no fueron entrenados en la política de la red.

La siguiente lista de temas debe ser cubierta cuando se desarrolla una PVA:

- ¿ Es permitido irrumpir en otra cuenta que no sea la propia?
- ¿ Es permitido descifrar password?
- ¿ Es permitido deteriorar el servicio?
- ¿ Se permitirá a los usuarios modificar archivos que no les pertenecen, aun si ellos tuvieran permisos de escritura?
- ¿ Podrán los usuarios compartir sus cuentas?

A menos de que se tengan una necesidad inusual, la respuesta a estas preguntas es No.

Es bueno agregar a las políticas una declaración concerniente a las licencias y derechos de software.

8.3.3 Determinar quien esta autorizado a conceder acceso y aprobar el uso

La política de seguridad deberá identificar quien está autorizado a conceder acceso a los servicios, además de determinar el tipo de acceso que puede conceder. De no suceder lo indicado, es difícil mantener un control de quien utiliza la red.

Al cumplir lo anterior, se pueden encontrar los tipos de accesos o controles que se han concedidos. Esto es útil para la identificación de las causas de agujeros de seguridad como resultado de la entrega de privilegios excesivos a usuarios.

Si a usuarios que se le han entregado privilegios, no son responsables y confiables, se corre el riesgo de crear agujeros de seguridad en el sistema y conceder privilegios inconsistentes a un usuario. Un sistema en esta situación regularmente dificulta su administración.

En una red, pueden existir un gran número de subredes y administradores de sistemas, lo cual dificulta el mantener un registro de los permisos que se han concedido a los recursos de la red. Se debe utilizar un sistema formal para los requerimientos de privilegios o permisos. Después de que

un usuario realiza una petición y que esta ha sido autorizada por un supervisor, el administrador del sistema deberá documentar las restricciones de seguridad o los accesos que se le han concedido al usuario.

8.3.4 Determinación de las responsabilidades de los usuarios

La política de seguridad debe definir los derechos y responsabilidades de los usuarios al utilizar los recursos y servicios de la red.

Se debe considerar temas concernientes a las responsabilidades de los usuarios.

- Directrices concernientes al uso de recursos de red como la restricción de usuarios y el tipo de restricciones.
- Que constituye abuso en términos de uso de los recursos de red y del funcionamiento de la red.
- Permitir o no a un usuario compartir su cuenta.
- ¿Un usuario podrá revelar su contraseña para acceder a una cuenta para permitir a otros usuarios trabajar en un proyecto?
- ¿Cuan frecuentemente los usuarios cambian sus contraseñas y otros requerimientos relacionados a ella?
- ¿Es responsable el usuario de proveer respaldo de su información o es responsabilidad del administrador?
- Repercusión para usuarios que revelen información propietaria.
- Acciones legales o castigos deben ser implementadas.
- Declaración de la privacidad de los correos electrónicos.
- Política concerniente a listas de correos, grupos de discusión.
- Política relacionada a la falsificación de e-mail.

La asociación de correos electrónicos (EMA), recomienda que se debe poseer una política sobre la protección de la privacidad de los miembros de una organización. La organización debe establecer políticas de privacidad que no limiten el correo electrónico. La asociación de correos electrónicos (EMA) sugiere cinco criterios para la evaluación de una política:

1. ¿La política cumple con la ley y con los deberes de terceros?
2. ¿Compromete la política innecesariamente el interés del trabajador, el empleador y a terceros?
3. ¿Es la política factible como un asunto práctico y probable de ser impuesta?
4. ¿La política tratará apropiadamente con las diferentes formas de comunicación y conservación de registro en una oficina?
5. ¿La política ha sido anunciada en acuerdo por todos los que les concierne?

8.3.5 Responsabilidades de los administradores de sistemas

La administradores de sistemas, recogen información contenida en los directorios privados de los usuarios para diagnosticar problemas de sistema. El usuario, por otra parte, tiene el derecho de mantener su privacidad, por consiguiente existe una interrelación entre los derechos de privacidad y las necesidades de los administradores de sistemas. Cuando se ha efectuado un ataque a la seguridad de la red, el administrador del sistema podrá tener la necesidad de obtener información de archivos del sistema, incluyendo los directorios raíces de los usuarios.

La política de seguridad deberá especificar el nivel al cual el administrador podrá examinar los directorios privados de un usuario para diagnosticar problemas del sistema e investigar las violaciones de seguridad.

Si la seguridad de la red está en riesgo, la política deberá permitir mayor flexibilidad a los administradores de los sistemas para corregir los problemas de seguridad. Se deben responder algunas preguntas a este respecto:

- ¿Puede el administrador del sistema monitorear o leer los archivos del usuario por alguna razón?
- ¿El administrador de la red tendrá el derecho de examinar el tráfico de la red o del servidor?
- ¿Que obligaciones tendrán los usuarios, administradores de sistemas y la organización para obtener acceso no autorizado a la información privada de otros individuos?

8.3.6 Manejo de información sensible

Se debe determinar que tipo de información sensible puede ser almacenada en un sistema específico. Desde el punto de vista de seguridad, información muy sensible como planillas de pago, calificaciones, investigaciones, deben ser restringidos a pocos servidores, por ende, a pocos administradores. Antes de considerar el conceder acceso a un usuario a un servicio en un servidor. Se debe considerar que información y servicios se a proporcionado al usuario para entregar más acceso. Si el usuario no tiene necesidad de trabajar con información sensible, el usuario no deberá tener acceso a una cuenta en el sistema que contenga ese material.

La seguridad de un sistema involucra hardware, software y costos de administración adicional.

8.4 Plan de acción cuando es violada la política de seguridad [2][6]

Cada vez que es violada la política de seguridad, el sistema queda abierto a amenazas de seguridad. Si no ocurre un cambio en la seguridad de la red cuando es violada la política de seguridad, deberá ser modificada la política de seguridad para remover aquellos elementos que no son seguros.

Independiente de que tipo de políticas es implementada, existe una tendencia de algunos usuarios a violar las políticas de seguridad.

Los procedimientos de seguridad que se implementen deben minimizar las posibilidades de violación sea indetectable. Al detectarse una violación a la política de seguridad, se debe clasificar si la violación a ocurrido debido a la negligencia de un usuario, accidente o error, ignorancia sobre la actual política, o por ignorar deliberadamente la política. En el último caso, la violación puede ser ejecutada por solo un individuo.

8.4.1 Respuesta a la violación de la política

Cuando ocurre una violación, la respuesta puede depender del tipo de usuario responsable de la violación. El responsable puede ser local o externo, determinando el tipo de respuesta que se puede generar ante la violación de seguridad. Estas pueden ser desde un advertencia o reprimenda verbal, una carta formal o presentando, hasta la presentación de una acusación legal.

Se deben definir las acciones basando en el tipo de violación. Deben ser claramente definidas, basadas en la clase de usuario que a violado la política de seguridad.

Tanto un usuario local como externo, deben estar advertidos de las políticas de seguridad.

El documento de la política de seguridad debe incluir procedimientos para manejar cada incidente de violación . Una apropiada bitácora debe ser mantenida y debe ser revisada periódicamente para observar alguna tendencia, ajustando la política de seguridad en caso de cualquier amenaza.

8.4.2 Respuesta de la violación de la política de seguridad por usuarios locales

Se pueden generar violaciones a la política de seguridad en la cual un usuario local viola la política, generando las siguientes situaciones:

- Un usuario local viola un sitio local.
- Un usuario local viola un sitio remoto.

En el primer caso, se puede tener mayor control sobre el tipo de respuesta sobre la violación. En el segundo caso, la situación es más compleja por el hecho de que otra organización es afectada, y cualquier respuesta que se tome debe ser discutida con la organización cuya seguridad ha sido violada.

8.4.3 Estrategia de respuesta

Existen dos tipos de estrategias de respuesta a incidentes que involucren la seguridad:

- Proteger y Proceder
- Perseguir y Acusar

Si el administrador de la política de seguridad siente que la organización es vulnerable, elegirá la estrategia de Protección y Proceder. La meta de esta política es proteger inmediatamente la red y restaurarla a su estado normal para poder continuar con su utilización. En el caso de no poder restaurar de inmediato, se debe aislar el segmento de red y apagar los sistemas con el objetivo de prevenir un mayor acceso no autorizado al sistema.

La segunda estrategia, Perseguir y Acusar, su principal objetivo es permitir al intruso seguir su acción, permitiendo vigilar sus acciones, sin que este se de cuenta de que esta siendo monitoreado. De esta forma se obtienen las pruebas necesarias para poder entablar una acusación legal. Esta ultima estrategia es la recomendada por las agencias de seguridad y la policía, ya que se obtiene los medios de prueba sin que el atacante se entere.

IV. CONCLUSIONES

Se concluye que para mantener la seguridad en una red, tanto domiciliaría como organizacional, se debe poseer conocimientos relacionados con los modelos que son la base de las comunicaciones. De esa forma se puede entender como esta compuesta una red de datos, la cual es la base de la inter-conectividad de redes, que en su conjunto es conocida como INTERNET. Estas redes, dentro del contexto mundial, corresponden a subredes de datos, las cuales dan acceso a millones de usuarios alrededor del planeta.

Las redes mencionadas son muy variadas en formas y tipos, esto basado en las tecnologías de hardware y software que las componen. Debido a las diferencias existentes entre los tipos de redes, debido a los tipos de hardware, sistemas operativos distintos e incompatibles entre ellos, es que se ha desarrollado protocolos comunes de comunicación. Estos protocolos tiene como fin poder generar la compatibilidad entre las diferentes redes imperantes en el planeta. Estos protocolos poseen fortalezas y debilidades, y son estas debilidades las que generan las oportunidades para que usuarios inescrupulosos tomen por asalto estas redes, generando los conocidos ataques informáticos. A estos usuarios de les conoce con los nombres de Crackers y Hackers, pero hay que dejar en claro que un Cracker es un usuario con intenciones maliciosas, entendiendo por ello cualquier tipo de acción que involucre la seguridad de la información que las redes poseen. Por otra parte, el Hacker, es un usuario que busca aumentar su conocimiento, investigando sistemas informáticos, buscando errores en las redes. De encontrarlos, estos hacen saber a los propietarios de las redes sus errores.

Es importante que un usuario sin mucho conocimiento informático, pueda familiarizarse con las topologías de redes, lo cual es un ordenamiento de las configuraciones físicas de las redes informáticas. Dependiendo de las topologías, los ataques pueden ser generados con mayor probabilidad de forma interna, sin olvidar la gravedad de ellos.

Para entender los tipos de ataques que se pueden sufrir, es necesario conocer y entender el concepto seguridad informática, y diferenciar los diferentes tipos de niveles de seguridad que existen. Estos niveles de seguridad, tiene como fin, entregar a un usuario las herramientas para saber cuanta seguridad es necesaria implementar, según los requerimientos que el usuario crea conveniente, después de evaluar los riesgos, el valor de la información y de las redes que desea proteger.

Al entender lo anterior, se puede conocer e identificar los bienes de información que son más relevantes para generar un mejor tipo de seguridad. Entender conceptos como bienes de información, identidad, confidencialidad, disponibilidad, entre muchos, es de vital importancia.

Una vez comprendidos estos conceptos, hay que conocer las formas por las cuales un atacante puede tomar control de sus sistemas. Conocer los métodos de espionaje, como Sniffers, Troyanos, etc., y sus usos, por sobre todo, identificar si se esta siendo atacado con algunas de esto es de vital importancia para detener los ataques y así proteger los bienes de información.

Si no se ha logrado detener la acción de algún método de espionaje, se debe identificar los probables ataques que se pueden sufrir, para tomar las medidas de protección necesarias para evitarlas. El comprender lo que se denomina Agujeros de Seguridad es de vital importancia, para poder evitarlos en los sistemas que el usuario utiliza.

Al haber comprendido todas las etapas anteriores, el usuario ya posee un conocimiento para implementar barreras de protección, mediante sistemas de hardware, softwares, o ambas. Estos sistemas, conocidos como Firewall, provén una protección contra los ataques de usuarios maliciosos. Estos firewalls, son configurados según el tipo de red que se desea proteger, además del valor de los bienes que se desean proteger. Bienes de información con costos mucho menores a muchas soluciones de seguridad conocidas, serian un gasto innecesario, debido a que recuperar la información tiene un costo mucho menor. Es por ello que siempre se debe crear una política de seguridad, la cual consiste en la creación de reglas y soluciones, tanto de hardware, software, y sobre todo, compromisos que los usuarios deben asumir para mantener la seguridad de los sistemas utilizados. Esto último es la base de una red segura, ya que si los usuarios no mantienen

normas estrictas, las redes, sin importar la cantidad de seguridad implementada, con el tiempo quedaran nuevamente al alcance de los atacantes. Es por ello que los usuarios deben de conocer las políticas de seguridad implantadas, para que no pasen de forma involuntaria a violarlas.

En el caso de una organización como las Universidades, donde se intercambia muchos tipos de información, desde información curricular, financiera, hasta información de tipo educativa, es importante poder distinguir los distintos tipos de usuarios, para así poder aislar sus redes, entregando diferentes tipos de accesos según sean los requerimientos. Es por ello que los administradores, deben tener clara sus políticas de seguridad, para así llevar un orden de los permisos ya concedidos, y así saber que otros permisos pueden conceder. Además, los administradores deben de conocer sus responsabilidades en relación a la política de seguridad, esto ya que son ellos quienes deben fiscalizar el buen uso de las redes de la organización para la cual trabajan.

Se concluye que es importante la responsabilidad de los usuarios en las redes informáticas, ya que la ignorancia de su utilización, y de las políticas de seguridad de las organizaciones, donde se encuentran ellas, generan las vulnerabilidades ante los ataques informáticos.

En el caso de usuarios domiciliarios, es difícil mantener un control por parte de los proveedores de conexión a Internet. Es por ello, que otros usuarios de estas redes, quedan indefensos frente a otros usuarios más experimentados que navegan por la red. Es por ello que el uso de al menos de el software Firewall de aplicación es muy conveniente, ya que crea una barrera entre los posibles atacantes y la información personal del usuario.

No hay que olvidar que el desarrollo de la ciencia y la técnica ha generado nuevos medios de transporte de la información, y es por ello que se han desarrollado tecnologías inalámbricas, las cuales han generado un desarrollo en los sistemas de seguridad. Routers inalámbricos han sido desarrollados, con un aumento en sus capacidades básicas de transmisión de datos, permitiendo la encriptación de datos (VPN), como también las posibilidades de filtraje de usuarios para acceder a las redes a las cuales están conectados, SPI, NAT, WEP, WAP.

Este trabajo entrega los fundamentos básicos para cualquier usuario básico en el uso de las redes informáticas, dando la posibilidad de que se obtengan los conocimientos necesarios para implementar métodos básicos de seguridad. Además, queda habilitado para aumentar sus conocimientos en áreas específicas de seguridad, como lo son los routers, firewall, etc.

Es necesario que las organizaciones implementen políticas de seguridad acorde a sus necesidades, capacitando a sus usuarios.

La seguridad, es uno de los temas más importantes en las redes informáticas, ya que la perdida de la información puede generar grandes daños económicos a organizaciones, como a usuarios domésticos.

Cualquier tipo de sistema de seguridad implementado, debe generar la disponibilidad y la seguridad de la información del usuario, ya que si no se estaría trasgrediendo algunos de los objetivos fundamentales de la seguridad informática, la disponibilidad, integridad, identidad, confidencialidad de la información.

V. REFERENCIAS BIBLIOGRAFICAS

[1] Andrew Tanenbaum , Redes de computadoras, 3ª edición, Ed. Prentice Hall Hispanoamericana, S.A, México, 1997, ISBN: 968-880-958-6

[2] Chris Hare, Siyan, Karanjit , Internet Firewalls and Network Security, 2nd Ed., New Rider Publishing, Indianapolis, USA, 1996

[3] Craig Zacker, Upgrading and Reparing Networks, Paul Doyle, Que Corporation, Indianapolis, USA, 1998, ISBN: 0-7897-0181-2

[4] Frederic Cooper, Implementing Internet Security, Ed. New Riders Publishing, Indianápolis, Indiana, U.S.A, 1995

[5] Mark Taber, Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network, Ed. Macmillan Computer Publishing, U.S.A, 2002

[6] Merike Kaeo, Designing Network Security, Ed. Cisco Press Publications, U.S.A, 1999

[7] Rob Scrimger, Kelli Adam, MCSE Training Guide: TCP/IP, 2nd Ed., New Rider Publishing, Indianapolis, USA, 1999

[8] E-Book, IP Routing Fundamental, Ed. Cisco Press Publications, U.S.A, 1999

[9] web.frm.utn.edu.ar/comunicaciones/modelo_osi.html#1

[10] www.drts-pr.com/Cedu5240/contenido/Topologias.html.#EmblemaCurso

[11] www.infospyware.com

[12] www.linksys.com/servlet/Satellite?childpagename=US%2FLayout&packedargs=c%3DL_Content_C1%26cid%3D1114037291212&pagename=Linksys%2FCommon%2FVisitorWrapper

[13] www.maestrosdelweb.com/editorial/ssniffers/

[14] www.maestrosdelweb.com/editorial/spyware/

[15] www.securityfocus.com/infocus/1549

[16] www.zonagratuita.com/a-curar/hacking/webspoofing.htm

ANEXO A

LISTADO DE PUERTOS USADOS POR TROYANOS

http://www.seguridadenlared.org/es/index5esp.html

puerto 1 (UDP) - Sockets des Troie
puerto 2 Death
puerto 15 B2
puerto 20 Senna Spy FTP server
puerto 21 Back Construction, Blade Runner, Cattivik FTP Server, CC Invader, Dark FTP, Doly Trojan, Fore, FreddyK, Invisible FTP, Juggernaut 42, Larva, MotIv FTP, Net Administrator, Ramen, RTB 666, Senna Spy FTP server, The Flu, Traitor 21, WebEx, WinCrash
puerto 22 Adore sshd, Shaft
puerto 23 ADM worm, Fire HacKer, My Very Own trojan, RTB 666, Telnet Pro, Tiny Telnet Server - TTS, Truva Atl
puerto 25 Ajan, Antigen, Barok, BSE, Email Password Sender - EPS, EPS II, Gip, Gris, Happy99, Hpteam mail, Hybris, I love you, Kuang2, Magic Horse, MBT (Mail Bombing Trojan), Moscow Email trojan, Naebi, NewApt worm, ProMail trojan, Shtirlitz, Stealth, Stukach, Tapiras, Terminator, WinPC, WinSpy
puerto 30 Agent 40421
puerto 31 Agent 31, Hackers Paradise, Masters Paradise
puerto 39 SubSARI
puerto 41 Deep Throat, Foreplay
puerto 44 Arctic
puerto 48 DRAT
puerto 50 DRAT
puerto 53 ADM worm, Lion
puerto 58 DMSetup
puerto 59 DMSetup
puerto 69 BackGate
puerto 79 CDK, Firehotcker
puerto 80 711 trojan (Seven Eleven), AckCmd, Back End, Back Orifice 2000 Plug-Ins, Cafeini, CGI Backdoor, Executor, God Message, God Message 4 Creator, Hooker, IISworm, MTX, NCX, Noob, Ramen, Reverse WWW Tunnel Backdoor, RingZero, RTB 666, Seeker, WAN Remote, Web Server CT, WebDownloader
puerto 81 RemoConChubo
puerto 99 Hidden
puerto, Mandragore, NCX
puerto 110 ProMail trojan
puerto 113 Invisible Identd Deamon, Kazimas
puerto 119 Happy99
puerto 121 Attack Bot, God Message, JammerKillah
puerto 123 Net Controller
puerto 133 Farnaz
puerto 137 Chode
puerto 137 (UDP) - Msinit, Qaz
puerto 138 Chode

puerto 139 Chode, God Message worm, Msinit, Netlog, Network, Qaz, Sadmind, SMB Relay
puerto 142 NetTaxi
puerto 146 Infector
puerto 146 (UDP) - Infector
puerto 166 NokNok
puerto 170 A-trojan
puerto 334 Backage
puerto 411 Backage
puerto 420 Breach, Incognito
puerto 421 TCP Wrappers trojan
puerto 455 Fatal Connections
puerto 456 Hackers Paradise
puerto 511 T0rn Rootkit
puerto 513 Grlogin
puerto 514 RPC Backdoor
puerto 515 lpdw0rm, Ramen
puerto 531 Net666, Rasmin
puerto 555 711 trojan (Seven Eleven), Ini-Killer, Net Administrator, Phase Zero, Phase-0, Stealth Spy
puerto 600 Sadmind
puerto 605 Secret Service
puerto 661 NokNok
puerto 666 Attack FTP, Back Construction, BLA trojan, Cain & Abel, lpdw0rm, NokNok, Satans Back Door - SBD, ServU, Shadow Phyre, th3r1pp3rz (= Therippers)
puerto 667 SniperNet
puerto 668 th3r1pp3rz (= Therippers)
puerto 669 DP trojan
puerto 692 GayOL
puerto 777 AimSpy, Undetected
puerto 808 WinHole
puerto 911 Dark Shadow, Dark Shadow
puerto 999 Chat power, Deep Throat, Foreplay, WinSatan
puerto 1000 Connecter, Der Späher / Der Spaeher, Direct Connection
puerto 1001 Der Späher / Der Spaeher, Le Guardien, Silencer, Theef, WebEx
puerto 1005 Theef
puerto 1008 Lion
puerto 1010 Doly Trojan
puerto 1011 Doly Trojan
puerto 1012 Doly Trojan
puerto 1015 Doly Trojan
puerto 1016 Doly Trojan
puerto 1020 Vampire
puerto 1024 Jade, Latinus, NetSpy, Remote Administration Tool - RAT [no 2]
puerto 1025 Fraggle Rock, md5 Backdoor, NetSpy, Remote Storm
puerto 1025 (UDP) - Remote Storm
puerto 1031 Xanadu
puerto 1035 Multidropper
puerto 1042 BLA trojan

puerto 1042 (UDP) - BLA trojan
puerto 1045 Rasmin
puerto 1049 /sbin/initd
puerto 1050 MiniCommand
puerto 1053 The Thief
puerto 1054 AckCmd
puerto 1080 SubSeven 2.2, WinHole
puerto 1081 WinHole
puerto 1082 WinHole
puerto 1083 WinHole
puerto 1090 Xtreme
puerto 1095 Remote Administration Tool - RAT
puerto 1097 Remote Administration Tool - RAT
puerto 1098 Remote Administration Tool - RAT
puerto 1099 Blood Fest Evolution, Remote Administration Tool - RAT
puerto 1104 (UDP) - RexxRave
puerto 1150 Orion
puerto 1151 Orion
puerto 1170 Psyber Stream Server - PSS, Streaming Audio Server, Voice
puerto 1174 DaCryptic
puerto 1180 Unin68
puerto 1200 (UDP) - NoBackO
puerto 1201 (UDP) - NoBackO
puerto 1207 SoftWAR
puerto 1208 Infector
puerto 1212 Kaos
puerto 1234 SubSeven Java client, Ultors Trojan
puerto 1243 BackDoor-G, SubSeven, SubSeven Apocalypse, Tiles
puerto 1245 VooDoo Doll
puerto 1255 Scarab
puerto 1256 Project nEXT, RexxRave
puerto 1269 Matrix
puerto 1272 The Matrix
puerto 1313 NETrojan
puerto 1337 Shadyshell
puerto 1338 Millennium Worm
puerto 1349 Bo dll
puerto 1386 Dagger
puerto 1394 GoFriller
puerto 1441 Remote Storm
puerto 1492 FTP99CMP
puerto 1524 Trinoo
puerto 1568 Remote Hack
puerto 1600 Direct Connection, Shivka-Burka
puerto 1703 Exploiter
puerto 1777 Scarab
puerto 1807 SpySender
puerto 1826 Glacier
puerto 1966 Fake FTP

puerto 1967 For Your Eyes Only - FYEO, WM FTP Server
puerto 1969 OpC BO
puerto 1981 Bowl, Shockrave
puerto 1991 PitFall
puerto 1999 Back Door, SubSeven, TransScout
puerto 2000 Der Späher / Der Spaeher, Insane Network, Last 2000, Remote Explorer 2000, Senna Spy Trojan Generator
puerto 2001 Der Späher / Der Spaeher, Trojan Cow
puerto 2023 Ripper Pro
puerto 2080 WinHole
puerto 2115 Bugs
puerto 2130 (UDP) - Mini Backlash
puerto 2140 The Invasor
puerto 2140 (UDP) - Deep Throat, Foreplay
puerto 2155 Illusion Mailer
puerto 2255 Nirvana
puerto 2283 Hvl RAT
puerto 2300 Xplorer
puerto 2311 Studio 54
puerto 2330 IRC Contact
puerto 2331 IRC Contact
puerto 2332 IRC Contact
puerto 2333 IRC Contact
puerto 2334 IRC Contact
puerto 2335 IRC Contact
puerto 2336 IRC Contact
puerto 2337 IRC Contact
puerto 2338 IRC Contact
puerto 2339 IRC Contact, Voice Spy
puerto 2339 (UDP) - Voice Spy
puerto 2345 Doly Trojan
puerto 2400 puertod
puerto 2555 Lion, T0rn Rootkit
puerto 2565 Striker trojan
puerto 2583 WinCrash
puerto 2589 Dagger
puerto 2600 Digital RootBeer
puerto 2702 Black Diver
puerto 2716 The Prayer
puerto 2773 SubSeven, SubSeven 2.1 Gold
puerto 2774 SubSeven, SubSeven 2.1 Gold
puerto 2801 Phineas Phucker
puerto 2929 Konik
puerto 2989 (UDP) - Remote Administration Tool - RAT
puerto 3000 InetSpy, Remote Shut
puerto 3024 WinCrash
puerto 3031 Microspy
puerto 3128 Reverse WWW Tunnel Backdoor, RingZero
puerto 3129 Masters Paradise

puerto 3131 SubSARI
puerto 3150 The Invasor
puerto 3150 (UDP) - Deep Throat, Foreplay, Mini Backlash
puerto 3456 Terror trojan
puerto 3459 Eclipse 2000, Sanctuary
puerto 3700 puertoal of Doom
puerto 3777 PsychWard
puerto 3791 Total Solar Eclypse
puerto 3801 Total Solar Eclypse
puerto 4000 Connect-Back Backdoor, SkyDance
puerto 4092 WinCrash
puerto 4201 War trojan
puerto 4242 Virtual Hacking Machine - VHM
puerto 4321 BoBo
puerto 4444 CrackDown, Prosiak, Swift Remote
puerto 4488 Event Horizon
puerto 4523 Celine
puerto 4545 Internal Revise
puerto 4567 File Nail
puerto 4590 ICQ Trojan
puerto 4653 Cero
puerto 4666 Mneah
puerto 4950 ICQ Trogen (Lm)
puerto 5000 Back Door Setup, BioNet Lite, Blazer5, Bubbel, ICKiller, Ra1d, Sockets des Troie
puerto 5001 Back Door Setup, Sockets des Troie
puerto 5002 cd00r, Linux Rootkit IV (4), Shaft
puerto 5005 Aladino
puerto 5010 Solo
puerto 5011 One of the Last Trojans - OOTLT, One of the Last Trojans - OOTLT, modified
puerto 5025 WM Remote KeyLogger
puerto 5031 Net Metropolitan
puerto 5032 Net Metropolitan
puerto 5321 Firehotcker
puerto 5333 Backage, NetDemon
puerto 5343 WC Remote Administration Tool - wCrat
puerto 5400 Back Construction, Blade Runner
puerto 5401 Back Construction, Blade Runner, Mneah
puerto 5402 Back Construction, Blade Runner, Mneah
puerto 5512 Illusion Mailer
puerto 5534 The Flu
puerto 5550 Xtcp
puerto 5555 ServeMe
puerto 5556 BO Facil
puerto 5557 BO Facil
puerto 5569 Robo-Hack
puerto 5637 PC Crasher
puerto 5638 PC Crasher
puerto 5742 WinCrash

puerto 5760 puertomap Remote Root Linux Exploit
puerto 5802 Y3K RAT
puerto 5873 SubSeven 2.2
puerto 5880 Y3K RAT
puerto 5882 Y3K RAT
puerto 5882 (UDP) - Y3K RAT
puerto 5888 Y3K RAT
puerto 5888 (UDP) - Y3K RAT
puerto 5889 Y3K RAT
puerto 6000 The Thing
puerto 6006 Bad Blood
puerto 6272 Secret Service
puerto 6400 The Thing
puerto 6661 TEMan, Weia-Meia
puerto 6666 Dark Connection Inside, NetBus worm
puerto 6667 Dark FTP, EGO, Maniac rootkit, Moses, ScheduleAgent, SubSeven, Subseven 2.1.4 DefCon 8, The Thing (modified), Trinity, WinSatan
puerto 6669 Host Control, Vampire
puerto 6670 BackWeb Server, Deep Throat, Foreplay, WinNuke eXtreame
puerto 6711 BackDoor-G, SubSARI, SubSeven, VP Killer
puerto 6712 Funny trojan, SubSeven
puerto 6713 SubSeven
puerto 6723 Mstream
puerto 6767 UandMe
puerto 6771 Deep Throat, Foreplay
puerto 6776 2000 Cracks, BackDoor-G, SubSeven, VP Killer
puerto 6838 (UDP) - Mstream
puerto 6883 Delta Source DarkStar (??)
puerto 6912 Shit Heep
puerto 6939 Indoctrination
puerto 6969 2000 Cracks, Danton, GateCrasher, IRC 3, Net Controller, Priority
puerto 6970 GateCrasher
puerto 7000 Exploit Translation Server, Kazimas, Remote Grab, SubSeven, SubSeven 2.1 Gold
puerto 7001 Freak88, Freak2k, NetSnooper Gold
puerto 7158 Lohoboyshik
puerto 7215 SubSeven, SubSeven 2.1 Gold
puerto 7300 NetMonitor
puerto 7301 NetMonitor
puerto 7306 NetMonitor
puerto 7307 NetMonitor, Remote Process Monitor
puerto 7308 NetMonitor, X Spy
puerto 7424 Host Control
puerto 7424 (UDP) - Host Control
puerto 7597 Qaz
puerto 7626 Binghe, Glacier, Hyne
puerto 7718 Glacier
puerto 7777 God Message, The Thing (modified), Tini
puerto 7789 Back Door Setup, ICKiller, Mozilla

puerto 7826 Oblivion
puerto 7891 The ReVeNgEr
puerto 7983 Mstream
puerto 8080 Brown Orifice, Generic backdoor, RemoConChubo, Reverse WWW Tunnel Backdoor, RingZero
puerto 8685 Unin68
puerto 8787 Back Orifice 2000
puerto 8812 FraggleRock Lite
puerto 8988 BacHack
puerto 8989 Rcon, Recon, Xcon
puerto 9000 Netministrator
puerto 9325 (UDP) - Mstream
puerto 9400 InCommand
puerto 9870 Remote Computer Control Center
puerto 9872 puertoal of Doom
puerto 9873 puertoal of Doom
puerto 9874 puertoal of Doom
puerto 9875 puertoal of Doom
puerto 9876 Cyber Attacker, Rux
puerto 9878 TransScout
puerto 9989 Ini-Killer
puerto 9999 The Prayer
puerto 10000 OpwinTRojan
puerto 10005 OpwinTRojan
puerto 10008 Cheese worm, Lion
puerto 10067 (UDP) - puertoal of Doom
puerto 10085 Syphillis
puerto 10086 Syphillis
puerto 10100 Control Total, GiFt trojan
puerto 10101 BrainSpy, Silencer
puerto 10167 (UDP) - puertoal of Doom
puerto 10520 Acid Shivers
puerto 10528 Host Control
puerto 10607 Coma
puerto 10666 (UDP) - Ambush
puerto 11000 Senna Spy Trojan Generator
puerto 11050 Host Control
puerto 11051 Host Control
puerto 11223 Progenic trojan, Secret Agent
puerto 11831 Latinus
puerto 12076 Gjamer
puerto 12223 Hack´99 KeyLogger
puerto 12310 PreCursor
puerto 12345 Adore sshd, Ashley, cron / crontab, Fat Bitch trojan, GabanBus, icmp_client.c, icmp_pipe.c, Mypic, NetBus, NetBus Toy, NetBus worm, Pie Bill Gates, ValvNet, Whack Job, X-bill
puerto 12346 Fat Bitch trojan, GabanBus, NetBus, X-bill
puerto 12348 BioNet
puerto 12349 BioNet, Webhead

puerto 12361 Whack-a-mole
puerto 12362 Whack-a-mole
puerto 12363 Whack-a-mole
puerto 12623 (UDP) - DUN Control
puerto 12624 ButtMan
puerto 12631 Whack Job
puerto 12754 Mstream
puerto 13000 Senna Spy Trojan Generator, Senna Spy Trojan Generator
puerto 13010 BitchController, Hacker Brasil - HBR
puerto 13013 PsychWard
puerto 13014 PsychWard
puerto 13223 Hack´99 KeyLogger
puerto 13473 Chupacabra
puerto 14500 PC Invader
puerto 14501 PC Invader
puerto 14502 PC Invader
puerto 14503 PC Invader
puerto 15000 NetDemon
puerto 15092 Host Control
puerto 15104 Mstream
puerto 15382 SubZero
puerto 15858 CDK
puerto 16484 Mosucker
puerto 16660 Stacheldraht
puerto 16772 ICQ Revenge
puerto 16959 SubSeven, Subseven 2.1.4 DefCon 8
puerto 16969 Priority
puerto 17166 Mosaic
puerto 17300 Kuang2 the virus
puerto 17449 Kid Terror
puerto 17499 CrazzyNet
puerto 17500 CrazzyNet
puerto 17569 Infector
puerto 17593 AudioDoor
puerto 17777 Nephron
puerto 18667 Knark
puerto 18753 (UDP) - Shaft
puerto 19864 ICQ Revenge
puerto 20000 Millenium
puerto 20001 Insect, Millenium, Millenium (Lm)
puerto 20002 AcidkoR
puerto 20005 Mosucker
puerto 20023 VP Killer
puerto 20034 NetBus 2.0 Pro, NetBus 2.0 Pro Hidden, NetRex, Whack Job
puerto 20203 Chupacabra
puerto 20331 BLA trojan
puerto 20432 Shaft
puerto 20433 (UDP) - Shaft
puerto 21544 GirlFriend, Kid Terror, Matrix

puerto 21554 Exploiter, FreddyK, Kid Terror, Schwindler, Winsp00fer
puerto 21579 Breach
puerto 21957 Latinus
puerto 22222 Donald Dick, Prosiak, Ruler, RUX The TIc.K
puerto 23005 NetTrash, Olive, Oxon
puerto 23006 NetTrash
puerto 23023 Logged
puerto 23032 Amanda
puerto 23321 Konik
puerto 23432 Asylum
puerto 23456 Evil FTP, Ugly FTP, Whack Job
puerto 23476 Donald Dick
puerto 23476 (UDP) - Donald Dick
puerto 23477 Donald Dick
puerto 23777 InetSpy
puerto 24000 Infector
puerto 24289 Latinus
puerto 25123 Goy\'Z TroJan
puerto 25555 FreddyK
puerto 25685 MoonPie
puerto 25686 MoonPie
puerto 25982 MoonPie
puerto 26274 (UDP) - Delta Source
puerto 26681 Voice Spy
puerto 27160 MoonPie
puerto 27374 Bad Blood, EGO, Fake SubSeven, Lion, Ramen, Seeker, SubSeven, SubSeven 2.1 Gold, Subseven 2.1.4 DefCon 8, SubSeven 2.2, SubSeven Muie, The Saint, Ttfloader, Webhead
puerto 27444 (UDP) - Trinoo
puerto 27573 SubSeven
puerto 27665 Trinoo
puerto 28431 Hack´a´Tack
puerto 28678 Exploiter
puerto 29104 NetTrojan
puerto 29292 BackGate
puerto 29369 ovasOn
puerto 29559 Latinus
puerto 29891 The Unexplained
puerto 30000 Infector
puerto 30001 ErrOr32
puerto 30003 Lamers Death
puerto 30005 Backdoor JZ
puerto 30029 AOL trojan
puerto 30100 NetSphere
puerto 30101 NetSphere
puerto 30102 NetSphere
puerto 30103 NetSphere
puerto 30103 (UDP) - NetSphere
puerto 30133 NetSphere

puerto 30303 Sockets des Troie
puerto 30700 Mantis
puerto 30947 Intruse
puerto 30999 Kuang2
puerto 31221 Knark
puerto 31335 Trinoo
puerto 31336 Bo Whack, Butt Funnel
puerto 31337 ADM worm, Back Fire, Back Orifice 1.20 patches, Back Orifice (Lm), Back Orifice russian, Baron Night, Beeone, bindshell, BO client, BO Facil, BO spy, BO2, cron / crontab, Freak88, Freak2k, Gummo, icmp_pipe.c, Linux Rootkit IV (4), Sm4ck, Sockdmini
puerto 31337 (UDP) - Back Orifice, Deep BO
puerto 31338 Back Orifice, Butt Funnel, NetSpy (DK)
puerto 31338 (UDP) - Deep BO, NetSpy (DK)
puerto 31339 NetSpy (DK), NetSpy (DK)
puerto 31557 Xanadu
puerto 31666 BOWhack
puerto 31745 BuschTrommel
puerto 31785 Hack´a´Tack
puerto 31787 Hack´a´Tack
puerto 31788 Hack´a´Tack
puerto 31789 (UDP) - Hack´a´Tack
puerto 31790 Hack´a´Tack
puerto 31791 (UDP) - Hack´a´Tack
puerto 31792 Hack´a´Tack
puerto 32001 Donald Dick
puerto 32100 Peanut Brittle, Project nEXT
puerto 32418 Acid Battery
puerto 32791 Acropolis
puerto 33270 Trinity
puerto 33333 Blakharaz, Prosiak
puerto 33567 Lion, T0rn Rootkit
puerto 33568 Lion, T0rn Rootkit
puerto 33577 Son of PsychWard
puerto 33777 Son of PsychWard
puerto 33911 Spirit 2000, Spirit 2001
puerto 34324 Big Gluck, TN
puerto 34444 Donald Dick
puerto 34555 (UDP) - Trinoo (for Windows)
puerto 35555 (UDP) - Trinoo (for Windows)
puerto 37237 Mantis
puerto 37266 The Killer Trojan
puerto 37651 Yet Another Trojan - YAT
puerto 38741 CyberSpy
puerto 39507 Busters
puerto 40412 The Spy
puerto 40421 Agent 40421, Masters Paradise
puerto 40422 Masters Paradise
puerto 40423 Masters Paradise
puerto 40425 Masters Paradise

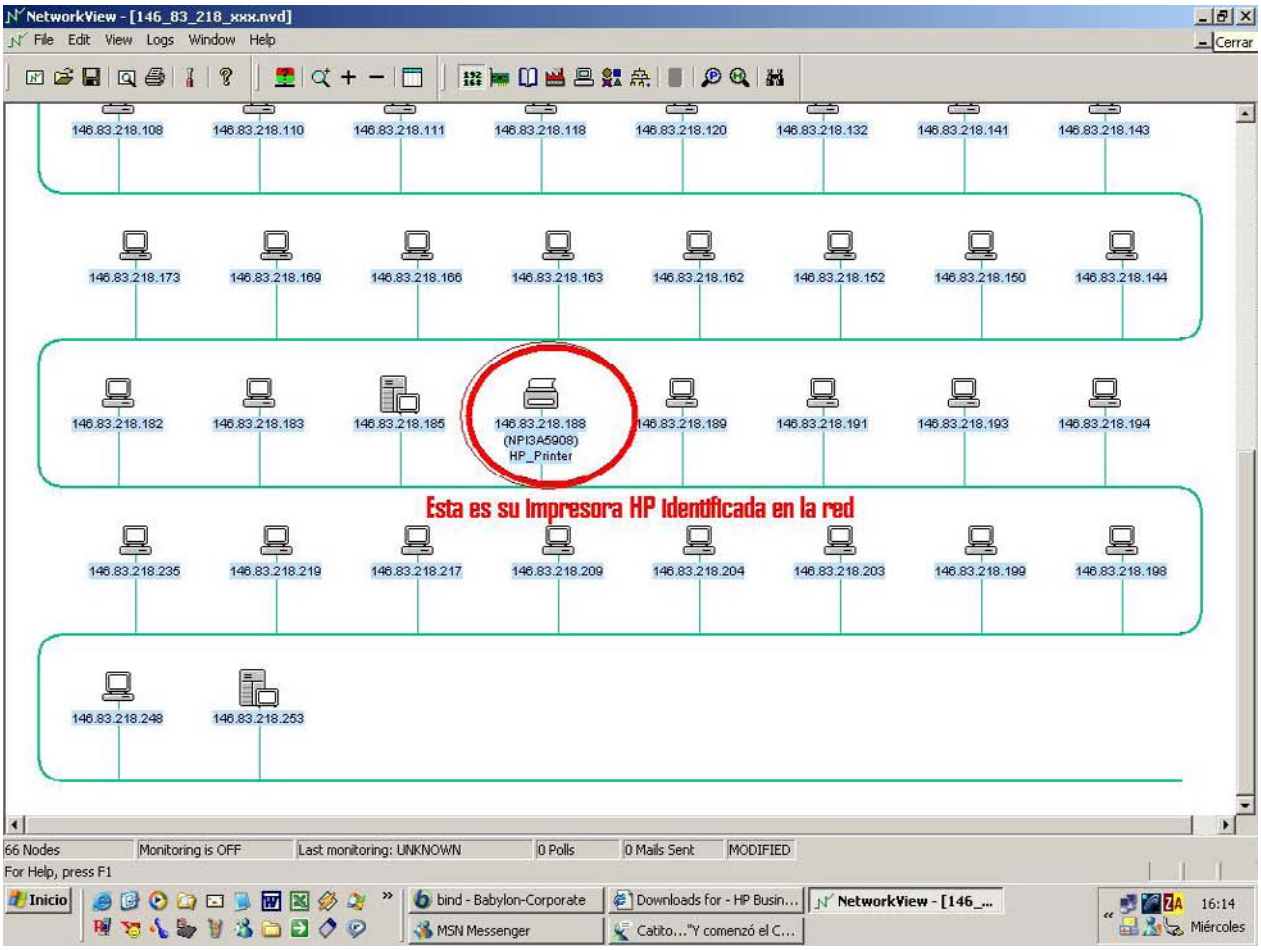
puerto 40426 Masters Paradise
puerto 41337 Storm
puerto 41666 Remote Boot Tool - RBT, Remote Boot Tool - RBT
puerto 44444 Prosiak
puerto 44575 Exploiter
puerto 44767 (UDP) - School Bus
puerto 45559 Maniac rootkit
puerto 45673 Acropolis
puerto 47017 T0rn Rootkit
puerto 47262 (UDP) - Delta Source
puerto 48004 Fraggle Rock
puerto 48006 Fraggle Rock
puerto 49000 Fraggle Rock
puerto 49301 OnLine KeyLogger
puerto 50000 SubSARI
puerto 50130 Enterprise
puerto 50505 Sockets des Troie
puerto 50766 Fore, Schwindler
puerto 51966 Cafeini
puerto 52317 Acid Battery 2000
puerto 53001 Remote Windows Shutdown - RWS
puerto 54283 SubSeven, SubSeven 2.1 Gold
puerto 54320 Back Orifice 2000
puerto 54321 Back Orifice 2000, School Bus
puerto 55165 File Manager trojan, File Manager trojan, WM Trojan Generator
puerto 55166 WM Trojan Generator
puerto 57341 NetRaider
puerto 58339 Butt Funnel
puerto 60000 Deep Throat, Foreplay, Sockets des Troie
puerto 60001 Trinity
puerto 60008 Lion, T0rn Rootkit
puerto 60068 Xzip 6000068
puerto 60411 Connection
puerto 61348 Bunker-Hill
puerto 61466 TeleCommando
puerto 61603 Bunker-Hill
puerto 63485 Bunker-Hill
puerto 64101 Taskman
puerto 65000 Devil, Sockets des Troie, Stacheldraht
puerto 65390 Eclypse
puerto 65421 Jade
puerto 65432 The Traitor (= th3tr41t0r)
puerto 65432 (UDP) - The Traitor (= th3tr41t0r)
puerto 65530 Windows Mite
puerto 65534 /sbin/initd
puerto 65535 Adore worm, RC1 trojan, Sins

ANEXO B

ATAQUE DoS IMPRESORA UACh

B.1 Escaneo Segmento Red UACh

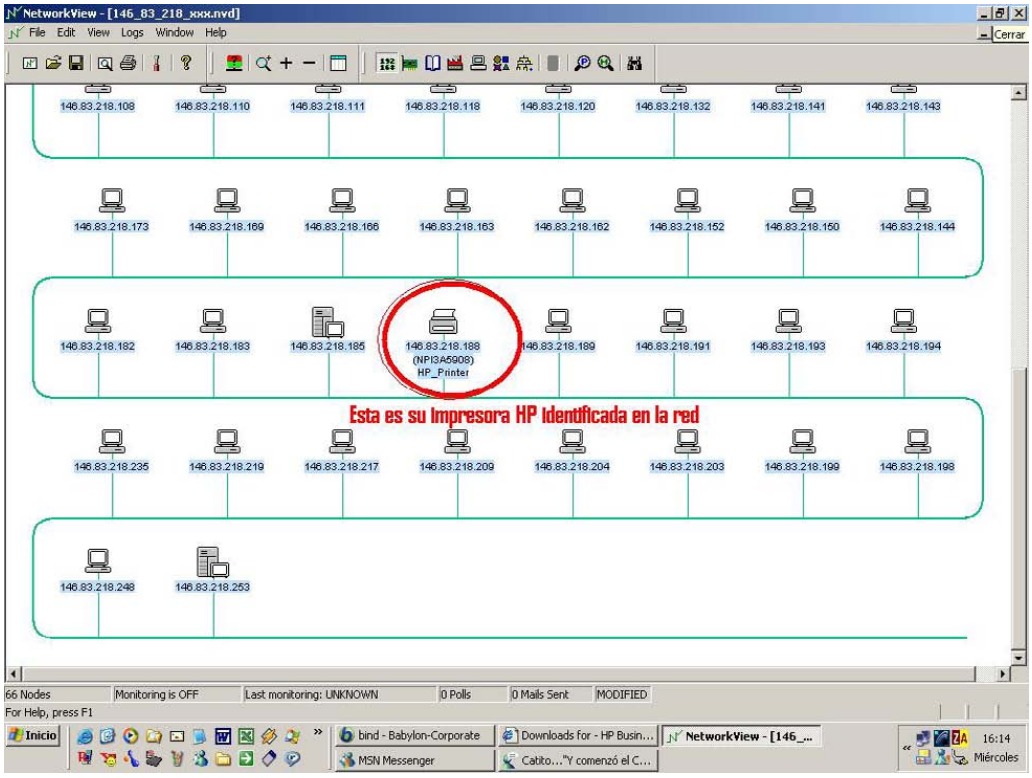
B.2 Identificación Impresora en Red



B.3 Aviso de Agujero de Seguridad y Ataque DoS a impresora en red.

Usted en este momento esta siendo parte de una prueba de seguridad de la red UACh.
Soy alumno tesista de la carrera de ingeniería electrónica, y estoy imprimiendo esta hoja en su impresora para infórmale que tiene un agujero de seguridad en ella. Le pido que se ponga en contacto conmigo Juan Ignacio Isla, fono:094100011, y con Luis Ampuero, patrocinador de mi tesis y además encargado de la red informática de la UACh, su fono es el 221086.
NO SE ASUSTE, ya que es una prueba, y la idea de esta es demostrar que UD puede sufrir un ataque desde dentro de la universidad, causándole a su impresora una sobrecarga de impresión, obligándola a que la desconecte de la red, lo que significaría para UD que pierda el servicio de impresión que tiene.
Le agradezco su tiempo y por favor le recuerdo que no tiene que preocuparse, esperamos poder pronto implementar políticas y medidas de seguridad. Recuerde que en la universidad , cualquier alumno puede realizar este tipo de ATAQUE. Le envió además un grafico donde se ve el escaneo de números IP realizados.
Le agradezco nuevamente su tiempo y buena disposición a mejorar la seguridad de los sistemas de la universidad. Por favor siga las instrucciones, contácteme y por nada del mundo bote esta impresión ya que es la prueba de haber recibido este ataque.

Atte
Juan Ignacio Isla



Valdivia, 25 de Agosto de 2004, 16:34 Hrs