VULNERAVILIDAD, TIPOS DE ATAQUES Y FORMAS DE MITIGARLOS EN LAS CAPAS DEL MODELO OSI EN LAS REDES DE DATOS DE LAS ORGANIZACIONES

Cesar Augusto Mejía Londoño
Nini Johana Ramírez Galvis
Juan Sebastián Rivera Cardona

UNIVERSIDAD TECNOLÓGICA DE PEREIRA
FACULTAD DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA, FÍSICA Y CIENCIAS DE LA COMPUTACIÓN
INGENIERÍA DE SISTEMAS Y COMPUTACIÓN
PEREIRA
2012

VULNERAVILIDAD, TIPOS DE ATAQUES Y FORMAS DE MITIGARLOS EN LAS CAPAS DEL MODELO OSI EN LAS REDES DE DATOS DE LAS ORGANIZACIONES

Cesar Augusto Mejía Londoño
Nini Johana Ramírez Galvis
Juan Sebastián Rivera Cardona

Proyecto de Grado

Profesor(a) Guía:
CARLOS AUGUSTO MENESES
Ingeniero de Sistemas

UNIVERSIDAD TECNOLÓGICA DE PEREIRA
FACULTAD DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA, FÍSICA Y CIENCIAS DE LA COMPUTACIÓN
INGENIERÍA DE SISTEMAS Y COMPUTACIÓN
PEREIRA
2012

AGRADECIMIENTOS Y DEDICATORIA

En primer lugar a Dios por ser nuestro guía espiritual y nuestro mentor en este camino que hemos recorrido.

A nuestros padres y hermanos que expresaron mediantes numerosas formas su apoyo incondicional.

A todos los maestros que a través de los años nos han transmitido el conocimiento con el cual nos podemos enfrentar a la vida y sobre todo a las adversidades.

A nuestro asesor del proyecto por el tiempo invertido y los excelentes aportes que dieron como logro la exitosa culminación de este proyecto.

Y por último pero no menos importante a la Universidad Tecnológica de Pereira, donde sus aulas de clase fueron gestoras del conocimiento

CONTENIDO

CONTENIDO DE ILUSTRACIONES

CONTENIDO DE TABLAS

GLOSARIO

ALGORITMO MD5: Algoritmo de Resumen del Mensaje 5, es un algoritmo de reducción criptográfico de 128 bits ampliamente usado.

AMENAZA: La causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

ATAQUE INFORMATICO: Es el método por el cual un individuo, mediante un sistema informático intenta tomar el control, desestabilizar o dañar otro sistema informático (ordenador, red privada, etc.).

BRUCE SCHEINER: Es un criptógrafo americano, especialista en seguridad informática, y escritor. El autor de varios libros de seguridad.

CISCO EXPRESS FORWARDING: Es una capa de avanzada tecnología de conmutación de 3 utiliza principalmente en las redes centrales de gran tamaño o de Internet, para mejorar el rendimiento global de la red.

SNMPSET: Comando que se utiliza para modificar realmente la información en la máquina remota.

COSTO: valor arbitrario, generalmente basado en el número de saltos, ancho de banda de los medios u otras medidas, que se asigna a través de un administrador

de red y que se usa para comparar varias rutas a través de un entorno de Internet work.

CRIPTOGRAFÍA: Actualmente se encarga del estudio de los algoritmos, protocolos y sistemas que se utilizan para proteger la información y dotar de seguridad a las comunicaciones y a las entidades que se comunican.

CRYPT (): Se utilizan para cifrar los datos.

DES (DATA ENCRYPTION STANDARD): Es un bloque de cifrado que utiliza el cifrado secreto compartido.

DIRECCIONAMIENTO LÓGICO: Se considera como la dirección IP y físico es una dirección que identifica una interfaz de red.

E-TAILING: Productos físicos que se venden al consumidor final apoyados en un sitio web; por ejemplo, venta de libros, videos, CD, DVD, autos, etc.

FIBRA MONOMODO: Es aquella donde el haz de luz solo viaja en un sentido.

FIBRA MULTIMODO: Es aquella en la que los haces de luz pueden circular por más de un modo o camino. Esto supone que no llegan todos a la vez.

FORWARDING: Se conoce como enrutamiento de Internet es un proceso utilizado para determinar la ruta que un paquete o datagrama puede ser enviado. El proceso utiliza la información de enrutamiento para tomar decisiones y está diseñado para enviar un paquete a través de redes múltiples.

FRAGMENTACIÓN IP: Es una técnica utilizada para dividir los datagramas IP en fragmentos de menor tamaño.

GATEWAYS O PUERTA DE ENLACE: Un nodo de red equipado para la interconexión con otra red que utiliza protocolos diferentes

GUSANO: Un gusano es un programa capaz de ejecutarse y programarse por sí mismo a través de redes, en ocasiones portando virus o aprovechando bugs de los sistemas a los que conecta para dañarlos.

HACKING: Hacking es un término usado para describir el acto de penetrar en un sistema informático cerrado para el conocimiento y la información que se contiene en su interior.

IMPACTO: "El impacto que una vulnerabilidad tiene en una organización es una medida del costo en el que incurre la misma, cuando decide no implementar las políticas de seguridad adecuadas, o cuando simplemente desconoce la existencia de la vulnerabilidad."[1]

INTER SWITCH LINK (ISL): Es un protocolo propietario de CISCO que mantiene información sobre VLANs en el tráfico entre Routers y Switches.

INTERNET SERVICE PROTOCOL (ISNS): Permite la detección automática, gestión y configuración de los dispositivos iSCSI y Fibre Channel

---

[1] JOLMAN, ALEXANDER. Seguridad Informática. [en línea.] < http://jrobledoherrera.blogspot.com/2009/02/seguridad-informatica.html>. [Citado el 25 de Febrero de 2012].

INTRUSIÓN: Es cualquier conjunto de acciones que comprometa la integridad, confidencialidad o disponibilidad de una información o un recurso informático.

IPCHAINS: Cadenas Cortafuegos IP de Linux, normalmente llamados ipchains, es un software gratuito para controlar los filtros de paquetes / cortafuegos capacidades en la serie 2.2 del kernel de Linux

IPSEC: Es la ONU Conjunto de Protocolos Cuya FUNCIÓN es asegurar las Comunicaciones Sobre el PROTOCOLO de Internet (IP) autenticando y / o cifrando Cada Paquete IP En Un flujo de Datos.

IRCS: Las redes de IRC consisten en grupos de servidores que están en contacto cercano con los demás. Los servidores en una red de mantener el contacto entre usted y todos los demás usuarios.

MACOF: Las inundaciones de la red local con direcciones MAC aleatorias.

MIB: Es una base de datos virtual que se usa para la gestión de las entidades en una red de comunicaciones

MICROSYSTEMS: Es una Cooperativa de Trabajo Asociado, del sector social y solidario, con actividad de servicios que busca satisfacer las necesidades y expectativas de productividad de las empresas.

NETBIOS: Es una especificación de interfaz para acceso a servicios de red, es decir, una capa de software desarrollado para enlazar un sistema operativo de red con hardware específico.

NETFILTER: Es un framework disponible en el núcleo Linux que permite interceptar y manipular paquetes de red. El componente más popular construido sobre Netfilter es iptables, una herramienta de cortafuegos que permite no solamente filtrar paquetes, sino también realizar traducción de direcciones de red (NAT) para IPv4 o mantener registros de log.

NETSTAT: Es una herramienta de línea de comandos que muestra un listado de las conexiones activas de una computadora, tanto entrantes como salientes.

NMAP: Es un programa de código abierto que sirve para efectuar rastreo de puertos escrito originalmente por Gordon Lyon (más conocido por su alias Fyodor Vaskovich). Se usa para evaluar la seguridad de sistemas informáticos, así como para descubrir servicios o servidores en una red informática.

NSLOOKUP: Es una administración de la red de línea de comandos disponibles para muchos sistemas operativos de computadoras, utilizado para consultar el Sistema de Nombres de Dominio (DNS) para obtener asignación de dirección IP.

PLAYLOAD: Es la parte de los datos transmitidos, que es el propósito fundamental de la transmisión, a la exclusión de la información que se envíe con ella (como los encabezados o metadatos, denominados a veces como los datos generales) únicamente a facilitar la entrega.

PLC (Programmable Logic Controller) o autómata programable es un equipo digital que se utiliza para la automatización de los procesos electromecánicos, tales como el control de la maquinaria en las líneas de montaje de fábrica, juegos mecánicos, o artefactos de iluminación.

PROTOCOLO IEEE 802.1Q: También conocido como dot1Q, fue un proyecto del grupo de trabajo 802 de la IEEE para desarrollar un mecanismo que permita a múltiples redes compartir de forma transparente el mismo medio físico, sin problemas de interferencia entre ellas (Trunking).

PROTOCOLOS AAA: El acrónimo AAA corresponde a un tipo de protocolos que realizan tres funciones: Autenticación, Autorización y Contabilización. La expresión protocolo AAA no se refiere pues a un protocolo en particular, sino a una familia de protocolos que ofrecen los tres servicios citados.

PROXY: Es un servidor (un sistema informático o una aplicación) que actúa como intermediario en las peticiones de los clientes que buscan recursos de otros servidores.

PS: Es un comando asociado en el sistema operativo UNIX que permite visualizar el estado de un Proceso.

RATIO: El Ratio de transmisión es el número de bits transmitidos en un segundo.

RED GALÁCTICA: Intergalactic Computer Network puede decirse que es la primera concepción de lo que eventualmente se convertiría en el Internet.

RED TELEFÓNICA CONMUTADA (RTC): Es una red de comunicación diseñada primordialmente para transmisión de voz, aunque pueda también transportar datos.

RFC 1157: Facilita el intercambio de información de administración entre dispositivos de red. Permite a los administradores supervisar el funcionamiento de la red

RFC 1446: Este RFC es un protocolo de normas de la IAB para la pista, comunidad de Internet, que solicita debate y sugerencias para mejoras.

RFC 2570: Es un protocolo estándar de Internet para la gestión de dispositivos en redes IP.

RFCs: Es un memorando publicado por el Internet Engineering Task Force (IETF), que describe los métodos, los comportamientos, la investigación, o las innovaciones aplicables al funcionamiento de la Internet y los sistemas conectados a Internet.

RIESGO: El riesgo es la posibilidad de sufrir algún daño o perdida en la información, estructura física y/o lógica del sistema, debido a un evento causado por un agente malintencionado.

RIP (ROUTER INFORMATION PROTOCOL): Es un protocolo de enrutamiento de vector de distancia, que emplea el número de saltos como métrica de enrutamiento.

RM -RF / &: Comando Unix que remueve o elimina un archivo

ROBERT MORRIS, JR: Es un científico de la computación estadounidense, conocido por haber creado el gusano de Morris en 1988, considerado como el gusano de la computadora por primera vez en Internet

RSTP: Es una versión mejorada del STP, el cual gestiona enlaces redundantes.

SCANLOGD: Es un puerto TCP herramienta de detección de exploración, que está diseñado para ser totalmente seguro de utilizar.

SCREENING ROUTERS: Un Router realiza detección de filtrado de paquetes y se utiliza como un servidor de seguridad.

SENDMAIL: Es un propósito general de correo electrónico interconexión de redes de enrutamiento instalación que soporta muchos tipos de correo electrónico de transferencia y entrega de métodos.

SEGURIDAD DE LA INFORMACIÓN: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden ser también consideradas.

SHELL: Es una pieza de software que proporciona una interfaz para los usuarios de un sistema operativo que proporciona acceso a los servicios de un núcleo.

SNORT: Es un Sniffer de paquetes y un detector de intrusos basado en red (se monitoriza todo un dominio de colisión).

SOCKET: Designa un concepto abstracto por el cual dos programas pueden intercambiar cualquier flujo de datos, generalmente de manera fiable y ordenada.

SOURCE-ROUTING: Permite un remitente de un paquete para especificar parcial o completamente la ruta que el paquete lleva a través de la red.

SSH: usa técnicas de cifrado que hacen que la información que viaja por el medio de comunicación vaya de manera no legible y ninguna tercera persona pueda descubrir el usuario y contraseña de la conexión ni lo que se escribe durante toda la sesión

SPAM: Término inglés coloquial muy utilizado para definir el envío indiscriminado de mensajes de correo electrónico no deseados.

STACK: Es una pila que puede tener cualquier tipo de datos abstracto como un elemento, pero se caracteriza por dos operaciones fundamentales, llamadas push y pop.

STREAMS: Proporcionan una forma de leer y escribir bytes desde y hacia un repositorio de seguridad

SYN: Es un bit de control dentro del segmento TCP, que se utiliza para sincronizar los números de secuencia iniciales ISN de una conexión en el procedimiento de establecimiento de tres fases.

TIME_WAIT: El socket está esperando después de cerrarse que concluyan los paquetes que siguen en la red.

TIMESTAMP: Es la hora a la que se registra un evento de un ordenador, no el tiempo del evento en sí.

TRAMAS: Nombre dado a las unidades de datos de la capa de enlace de datos, una trama es la encapsulación de un paquete.

UCLA: Donde Kleinrock creó el Centro de medición de red. Un ordenador SDS Sigma 7 fue el primero en conectarse.

UNICAST RPF: Tal como se define en el RFC 3704 es una evolución del concepto de que el tráfico de las redes conocidas no válidos no deben ser aceptados en las interfaces de las que nunca deberían haberse originado.

URG: Puntero de urgencia válido (Indica un offset a añadir al nº de secuencia)

VIRUS: Un virus es una secuencia de código que se inserta en un fichero ejecutable (denominado huésped), de forma que cuando el archivo se ejecuta, el virus también lo hace, insertándose a sí mismo en otros programas.

VULNERABILIDAD: Las vulnerabilidades pretenden descubrir las debilidades y los métodos más comunes que se utilizan para perpetrar ataques a la seguridad de la familia de protocolos TCP/IP (confidencialidad, integridad y disponibilidad de la información).

INTRODUCCIÓN

Todo administrador de una red o de sistemas de información, es responsable de la integridad tanto de la información pertinente de una organización como de la red misma, sin embargo tanto los sistemas de información como las redes han traído consigo un montón de vulnerabilidades, las cuales se han intentado disminuir, pero muchas veces no se tiene los conocimientos suficientes, por lo tanto las medidas que se toman pueden ser superficiales.

Esto hace que se incurra en costos financieros y en el tiempo que una organización debe invertir para evitar los ataques o intrusiones de terceros. Es importante reconocer que existen diferentes amenazas, riesgos y vulnerabilidades a las que están expuestas las organizaciones en sus sistemas de comunicaciones y se debe encontrar la forma más profunda de reducir dichas vulnerabilidades, además de diferenciar los tipos de ataque y la forma en que operan.

El desarrollo de este documento pretende servir de información para cualquier administrador de red o persona que pretenda tener un conocimiento sobre debilidades en las redes y que por medio de estas se puede afectar la integridad, ya sea de organizaciones o individuos que hagan de la información parte de la cotidianidad de sus días.

Para darle un enfoque ordenado a este conocimiento, el documento basa su estructura en cinco capítulos, planteando ideas escalonadas que van desde la descripción del modelo OSI hasta las propuesta para solucionar un problema que

surge de las redes de datos, que evoluciona con el tiempo y el avance de la tecnología.

El primer capítulo describe la razón de ser del documento, planteando los problemas que se pueden presentar en las organizaciones que no tenga noción de cuan vulnerable puedan ser sus datos y sus equipos de comunicación o de cómputo dentro de un sistema de información.

El segundo capítulo define las características del modelo OSI, las normas, los dispositivos mediante el cual se basa el funcionamiento de muchas redes de datos y por el cual se guían los intrusos para tener acceso a los sistemas que ellos deseen atacar.

El tercer capítulo hace mención a los ataques que atentan contra las falencias del modelo OSI además de hablar sobre políticas de seguridad que se deben aplicar para disminuir estas intrusiones.

También, se hace un análisis de los ataques y como estos afectan los procesos de las organizaciones, denotando el impacto operacional de estos. Por último se realiza un análisis de la prevención, detección y mitigación de las principales vulnerabilidades y ataques centrado en la red de datos de toda la organización.

GENERALIDADES

1.1 PLANTEAMIENTO DEL PROBLEMA

La seguridad es algo primordial en el correcto funcionamiento de las redes de datos, pues con ella se garantiza la confidencialidad, la estabilidad, y la convergencia de datos sobre un mismo medio, sin mencionar otros. Una violación a dicha seguridad puede ocasionar severos daños a la integridad de las redes de datos, las cuales son de vital importancia en cualquier organización y pueden llegar a afectar datos relevantes para usuarios que hagan uso de diferentes sistemas de información.

La omisión de las políticas de seguridad puede ocasionar que los datos terminen en manos de individuos inescrupulosos que los manipulen con intenciones negativas. Existen múltiples mecanismos de seguridad que permiten mitigar los ataques a los sistemas de información, sin embargo no son cien por ciento confiables.

Se plantea entonces una necesidad de identificar las falencias y vulnerabilidades de las empresas y a qué tipo de ataques se ven expuestas en sus sistemas de comunicaciones, para poder dar posibles soluciones, prevenirlos o mitigarlos.
En la medida que las empresas tengan conocimiento de los ataques informáticos. ¿Cómo podrían prevenir y mitigar dichas vulnerabilidades?

1.2 JUSTIFICACIÓN

En vista de la importancia que han tomado las redes de datos en los entornos organizacionales se pretende que este documento sirva como medio de consulta para servir de apoyo en la implementación de nuevos sistemas de seguridad.

1.2.1 ENTORNO CIENTIFICO

Muchas organizaciones, personas o administradores en el área de sistemas ven únicamente la parte superficial de lo que son las vulnerabilidades y los ataques sobre los sistemas de información; veneran los antivirus, y los firewalls como típicos medios de prevención ante los posibles y diferentes entes que amenazan los datos, pudiendo desconocer cuál es la realidad de fondo.

Esta investigación tiene como meta recopilar información que les permita a aquellos administradores o usuarios que velan por la seguridad de los sistemas de información ampliar la visión que se tiene sobre el modelo OSI y donde se encuentran sus debilidades.

1.2.2 ENTORNO ECONÓMICO

Muchas empresas de acuerdo a su actividad económica sobre todo aquellas que tienen que ver con sistemas de información hacen grandes inversiones en el diseño e implementación de infraestructuras de red que les permita mantener sus datos de forma confiable e íntegra además de segura en sus repositorios.

Sin embargo los ataques a las redes son un tema que evoluciona con el pasar del tiempo, haciendo que las empresas sigan invirtiendo en soluciones para prevenir esos ataques ya sea comprando nuevos antivirus, o las actualizaciones de estos, o recurriendo a la adquisición de nuevos equipos de seguridad que acarrean un costo adicional. No obstante el costo de los equipos adquiridos se hace insignificante ante el valor que podría representar la perdida de los datos que son el activo más importante que tiene una empresa.

Implícitamente, el proyecto muestra un panorama donde se evidencia la problemática económica en las organizaciones donde muchas veces no se mide el costo que podría provocar la pérdida de información valiosa.

1.2.3 ENTORNO SOCIAL

La información y los datos son un concepto que se ha empleado desde los inicios de la humanidad y con las cuales en la actualidad las organizaciones e individuos comparten ideas y en su defecto, desarrollan sus actividades.
Sin embargo, los avances tecnológicos han transformado los métodos de manipulación, permitiendo más agilidad al acceso de los datos, pero con los

avances tecnológicos también ha llegado a la mente de sujetos inescrupulosos el deseo de obtener la información de muchas compañías con fines no muy sanos para la sociedad o para la misma compañía, es por lo tanto indispensable mantener dichos datos completamente confidenciales y seguros.

La manipulación inadecuada de la información confidencial de las organizaciones o individuos puede acarrear problemas sociales, perturbando la intimidad y el libre desarrollo de la personalidad, además de la presentación de posibles plagios dando origen a una competencia desleal.

1.3 OBJETIVOS

1.3.1 OBJETIVO GENERAL

Realizar una monografía para determinar los tipos de ataques a las capas del modelo OSI y las formas de mitigarlos en empresas que poseen infraestructura de comunicaciones y su posible impacto.

1.3.2 OBJETIVOS ESPECÍFICOS

- Analizar el funcionamiento de las 7 capas del modelo OSI
- Identificar qué tipo de ataques se presentan relacionados con las diferentes capas del modelo OSI.
- Encontrar las vulnerabilidades que tienen las organizaciones en sus sistemas de comunicaciones.
- Identificar el impacto operacional por fallas en los sistemas de información y comunicaciones de una organización.
- Relacionar las diferentes formas de prevención a los diversos ataques a las infraestructuras de red

1.4 ANTECEDENTES

Las vulnerabilidades de las redes aumentan en la medida que no se toman las debidas precauciones y cuando se tienen malos hábitos a la hora de configurar ciertos aspectos de una red. Esto se puede apreciar en las Arquitecturas Inseguras, Redes de Difusión y los Servidores Centralizados.

1.4.1 ARQUITECTURAS INSEGURAS

Una red mal configurada es un punto de entrada principal para usuarios no autorizados. Al dejar una red local abierta, confiable, vulnerable a la Internet que es altamente insegura, es casi como que dejar una puerta abierta en un vecindario con alta criminalidad, puede que no ocurra nada durante un cierto tiempo, pero eventualmente alguien intentará aprovecharse de la oportunidad.

1.4.2 REDES DE DIFUSION

Los administradores de sistemas a menudo fallan al no darse cuenta de la importancia del hardware de la red en sus esquemas de seguridad. El hardware simple, tal como concentradores y enrutadores a menudo se basan en broadcast (difusión) o en el principio de “sin-interruptores”; esto es, cada vez que un nodo

transmite datos a través de la red a un nodo receptor, el concentrador o enrutador hace una difusión de los paquetes de datos hasta que el nodo destino recibe y procesa los datos.

Este método es vulnerable para hacer engaños de direcciones (Spoofing) al protocolo de resolución de direcciones *ARP* (Address Protocol Resolution) o control de acceso al medio *MAC* (Media Access Control) tanto por intrusos externos como por usuarios no autorizados.

1.4.3 SERVIDORES CENTRALIZADOS

Otra falla potencial de redes es el uso de computación centralizada. Una forma común de reducir costos para muchos negocios es el de consolidar todos los servicios a una sola máquina poderosa. Esto puede ser conveniente porque es fácil de manejar y cuesta considerablemente menos que una configuración de múltiples servidores. Sin embargo, un servidor centralizado introduce un punto único de falla en la red. Si el servidor central está comprometido, puede dejar la red totalmente inútil o peor aún, sensible a la manipulación o robo de datos. En estas situaciones un servidor central se convierte en una puerta abierta, permitiendo el acceso a la red completa.

MARCO TEÓRICO Y NORMAS

2.1 NORMAS DE SEGURIDAD DE LA INFORMACIÓN

2.1.1 NORMA ISO 17799

"Debido a la necesidad de hacer segura la información que poseen las organizaciones era necesaria la existencia de alguna normativa o estándar que acogiera todos los aspectos a tener en consideración por parte de las organizaciones para protegerse eficientemente frente a todos los probables incidentes que pudieran afectarla por esta necesidad apareció el BS 7799, o estándar para la gestión de la seguridad de la información, el cual es un estándar desarrollado por el British Standard Institute en 1999 en el que se engloban todos los aspectos relacionados con la gestión de la seguridad de la información dentro de la organización. Esta normativa británica acabó desembocando en la actual ISO/IEC 17799:2000 – Code of Practice Information Security Management."[2]

ISO/IEC 17799 (también ISO 27002) es un estándar para la seguridad de la información publicado por primera vez como ISO/IEC 17799:2000 por la International Orgnization For Standardization y por la Comisión International Electrotechnical Commission en el año 2000 y con el título de Information Technology - Security Techniques - Code of Practice For Information Security management. La actualización de los contenidos del estándar se publicó en el año 2005 el documento actualizado denominado ISO/IEC 17799:2005.

---

[2] JOLMAN, ALEXANDER. Seguridad Informática. [en línea.] < http://jrobledoherrera.blogspot.com/2009/02/seguridad-informatica.html>. [Citado el 25 de Febrero de 2012].

2.1.2 ISO/IEC 27001 SEGURIDAD DE LA INFORMACIÓN

"Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un *Sistema de Gestión de la Seguridad de la Información* (SGSI) según el conocido "Ciclo de Deming": PDCA - acrónimo de Plan, Do, Check, *Act* (Planificar, Hacer, Verificar, Actuar). Es consistente con las mejores prácticas descritas en ISO/IEC 17799 (actual ISO/IEC 27002) y tiene su origen en la norma BS 7799-2:2002, desarrollada por la entidad de normalización británica, la British Standards Institution (BSI)."[3]

"La información tiene una importancia fundamental para el funcionamiento y quizá incluso sea decisiva para la supervivencia de la organización. El hecho de disponer de la certificación según ISO/IEC 27001 ayuda a gestionar y proteger los valiosos activos de información.

ISO/IEC 27001 es la única norma internacional auditable que define los requisitos para un sistema de gestión de la seguridad de la información (SGSI). La norma se ha concebido para garantizar la selección de controles de seguridad adecuados y proporcionales.
Ello ayuda a proteger los activos de información y otorga confianza a cualquiera de las partes interesadas, sobre todo a los clientes. La norma adopta un enfoque

[3] ISO (INTERNATIONAL ORGANIZATION OF ESTANDARDIZATION). ISO/IEC 27001:2005. [en línea]. <http://www.iso.org/iso/catalogue_detail?csnumber=42103>. [Citado el 28 de Febrero de 2012].

por procesos para establecer, implementar, operar, supervisar, revisar, mantener y mejorar un SGSI."[4]

[4] BSI (British Standards Institution 2012). Seguridad de la Información ISO/IEC 27001. [en línea.] <http://www.bsigroup.es/certificacion-y-auditoria/Sistemas-de-gestion/estandares-esquemas/Seguridad-de-la-Informacion-ISOIEC27001/> [Citado el 28 de Febrero de 2012].

2.2 MARCO TEORICO

La evolución de las redes es un concepto que a lo largo de su existencia ha presentado cambios considerables, debido al avance de la ciencia que se ha extendido a través del tiempo, seguramente esto no va a parar aquí, ya que a diario se sigue avanzando en el conocimiento permitiendo darle un nuevo horizonte a las tecnologías.

Con estos conocimientos adquiridos se ha logrado mejorar muchos aspectos acerca de las redes de comunicaciones, como: confidencialidad, integridad y disponibilidad (3 aspectos de los cuales se explicará más adelante en profundidad), además de mejorar características como lo velocidad.

En el desarrollo del documento se explicara algunos conceptos relevantes acerca de las redes de comunicación.

2.2.1 TEORIA GENERAL DE REDES DE DATOS

2.2.1.1 RED DE COMUNICACIONES

“Una red de comunicaciones es un conjunto de medios técnicos que permiten la comunicación a distancia entre equipos autónomos (no jerárquica -master/slave-).

Normalmente se trata de transmitir datos, audio y vídeo por ondas electromagnéticas a través de diversos medios (aire, vacío, cable de cobre, fibra óptica, etc.).

La información se puede transmitir de forma analógica, digital o mixta, pero en cualquier caso las conversiones, si las hay, siempre se realizan de forma transparente al usuario, el cual maneja la información de forma analógica exclusivamente.

Las redes más habituales son las de ordenadores, las de teléfono, las de transmisión de audio (sistemas de megafonía o radio ambiental) y las de transmisión de vídeo (televisión o vídeo vigilancia)."[5]

2.2.1.2 TIPOS DE REDES DE COMUNICACIONES

De acuerdo a [19] las redes se clasifican de diferentes maneras, entre las principales se tienen:

- Por su extensión: Redes de área personal (PAN), local (LAN), extensa (WAN)
- Por su topología: Estrella, bus, anillo, malla, mixta.
- Por su conexión física: redes punto a punto, multipunto o de difusión.
- Por su técnica de transmisión de datos: líneas dedicadas, circuito conmutado o paquetes conmutados.
- Por su uso: se clasifican en redes privadas o corporativas y redes públicas.

[5] MONTAÑANA, Profesor. Redes de Comunicaciónes. Madrid: Güimi, 2009. p.4, 6 - 9

a) *Por su topología*

Se debe tener en cuenta la diferencia que existe entre una topología física (Es la forma en la que el cableado se realiza en una red) y topología lógica (es el funcionamiento de la red para que sea más eficiente).

La topología física de una red define únicamente la distribución del cable que interconecta los diferentes ordenadores. Las más utilizadas son bus, estrella y anillo.

Ilustración 1: Topologías de Red

Fuente: Los Autores.

b) *Por su Conexión Física*

Redes punto a punto (Unicast): Esta es un tipo de arquitectura de red y es una conexión en la cual solo participan dos nodos, donde los dispositivos interactúan como colega, es decir, cualquiera puede tomar el papel de maestro o esclavo.
Se pueden clasificar en tres tipos, según el sentido de las comunicaciones que transportan:

- *Simplex:* solo se hace la transacción en una sola trayectoria
- *Semi-dúplex (Half-duplex)*: envía datos en ambos sentidos, pero uno a la vez.
- *Dúplex (Full-duplex)*: envía datos en los dos sentidos simultáneamente.

Redes multipunto o redes de difusión (Broadcast): es una conexión en la que varios elementos están conectados en un mismo medio, basadas principalmente en bus compartido y redes inalámbricas. La información fluye de forma bidireccional y es accesible para todas las terminales de la red.
No se podrá garantizar la confidencialidad, Sin importar que tipo de emisión marcada es: como Unicast, Multicast o Broadcast.

c) *Por su Técnica de Transmisión de Datos*

Líneas dedicadas: Enlace punto a punto permanente y siempre disponible, estas posibilitan la transmisión de datos a velocidades medias y altas (de 64Kbps a 140 Mbps). Son usadas en su mayoría por las redes WAN con la velocidad que fije el proveedor, y por lo regular son simétricas y full-duplex. Estas redes tienen un costo alto, teniendo en cuenta que son para una gran cantidad de tráfico continuo.
Modelos de circuito conmutado (Circuit Switching): En este modelo no se comparte los medios, cuando comienza la transmisión se conservan los recursos

intermedios que se requieren para establecer y mantener el circuito, llegando a cortarse el canal de comunicación.
Los dispositivos mantienen información sobre el estado de la comunicación (statusfull) aplicado en la *Red Telefónica Conmutada (RTC4)* incluyendo:

- *Red Telefónica Básica (RTB)*
- *Red Digital de Servicios Integrados (RDSI o ISDN)*
- *GSM (Global System for Mobile Comunications)*

Cuando se determina el circuito, éste se manifiesta como una línea dedicada ofreciendo un transporte físico de bits en el cual se puede manejar cualquier protocolo de nivel de enlace. En cuanto al costo es proporcional a la distancia y tiempo de conexión.

Modelos de paquetes conmutados (Packet Switching): Este modelo se divide en paquetes que comparten los medios. Es posible utilizar varios enlaces en cada interfaz físico.
Existen dos Submodelos:

- *Datagramas:* Cada uno de los paquetes debe estar plenamente delimitado e identificado, debe llevar con él la dirección de destino y cada paquete sabe cuál es su camino, sin necesidad que el origen y destino se comuniquen previamente. Este tipo de modelo no garantiza que lleguen todos los paquetes o que van a llegar en orden, incluso si van a tener errores. Los dispositivos no poseen información acerca del estado de la comunicación.

- *Circuitos virtuales (VC: Virtual Circuit):* Simula un circuito conmutado, pero compartiendo los medios. Lo Primero que hace es establecer conexión y los

equipos intermedios conservan una porción de sus recursos, luego los demás paquetes siguen el mismo camino en orden. Este modelo es principalmente usado en telefonía digital y redes como ATM.

d) Por su Cobertura

Redes de área local (LAN):

Es una red de propiedad privada que tiene un alcance de unos cuantos kilómetros de distancia, alrededor de 200 metros, pero podría llegar a un kilómetro de distancia con repetidores, como por ejemplo un edificio, una oficina o un centro educativo.

Esta red es utilizada para interconectar computadoras personales o de oficinas, que tienen como objetivo compartir los recursos y la información. Pero de igual manera están limitadas en tamaño, por lo que el tiempo de transmisión no es el mejor. Estas redes cuentan con un bajo retardo y son muy escasos los errores.

También utilizan tecnología de difusión por medio de un cableado simple con el cual están conectados todos los equipos. Operan a velocidades entre 10 y 100 Mbps.

Redes de área extensa (WAN)

Este tipo de red es usada habitualmente por proveedores o también llamados ISP (Internet Service Provider), estas en principio se usaban básicamente para transmisión de voz por las empresas de telefonía, en la actualidad hacen parte de redes que tienen como función transmitir de datos adicional a la voz.

[6]

En un principio este tipo de redes eran reconocidas por su baja velocidad, alta tasa de errores y su alto costo. Aunque el costo sigue siendo alto hoy en dia estas redes han mejorado sus características permitiendo más fiabilidad y velocidad.

2.2.1.3 HISTORIA Y UTILIDAD DE LAS REDES EN LAS ORGANIZACIONES

Según [20] desde los años sesenta las organizaciones han ido creciendo de forma exponencial, pasando de simples negocios de familia con ubicación estática a industrias gigantes llenas de filiales regadas por todo el mundo que requieren de especial cuidado para el manejo de sus datos confidenciales.

El concepto de una red de computadoras capaz de comunicar usuarios en distintas computadoras fue formulado por J.C.R. Licklider de Bolt, Beranek and Newman (BBN) en agosto de 1962, en una serie de notas que discutían la idea de *"Red Galáctica*". Licklider fue convocado por ARPA (Agencia de Investigación de Proyectos Avanzados) perteneciente al Departamento de Defensa de los Estados Unidos para la ejecución de su proyecto con fines militares. Las ideas principales de esta investigación consistían en:

- El uso de una red descentralizada con múltiples caminos entre dos puntos.

- La división de mensajes completos en fragmentos que seguirían caminos distintos. La red estaría capacitada para responder ante sus propios fallos.

De esta idea[6] surgió el ARPANET que en 1969 transmitió sus primeros mensajes y pudo conectar las universidades de STANFORD y la *UCLA.* ARPANET utilizaba una serie de pequeños ordenadores denominados Procesadores de la Interfaz de Mensajes (IMPs), los cuales implementaban la técnica de almacenar y reenviar y utilizando un módem telefónico para conectarse a otros equipos (a una velocidad de 50 kbits por segundo). Los ordenadores centrales se conectaban a los IMPs mediante interfaces en serie a la medida.

---

[6] BOLT BERANEK y NEWMAN INC ARLINGTON VA, A History of the ARPANET: The First Decade. 1981

Desde la primitiva ARPANET se empezó a utilizar e implementar las redes que se caracterizaban por su descentralización pues sus nodos estaban regados y propagados por toda la topología además de poder dividir los mensajes en fragmentos que pudieran ir por diferentes rutas y juntarse en el destino permitiendo así un adecuado manejo de errores.

Actualmente las organizaciones ya han utilizado varios modelos de red y se han robustecido las ideas ya mencionadas por medio de la implementación de protocolos que han facilitado y optimizado la trasmisión de información a través de las redes de datos.

Para una organización sumergida en la era de la información, la necesidad de tener toda una infraestructura de comunicaciones es fundamental para el correcto funcionamiento de la misma, puesto que el mundo empresarial moderno se globalizó a tal punto que la información se maneja de igual forma en muchos lugares de la tierra. Pero, porque es esencial para una organización la utilización e implementación de las redes de comunicaciones para su correcto funcionamiento? a continuación algunas razones:

- Publicidad constante
- Reducción de costos en estudios de mercado.
- No existen los límites geográficos ni de tiempo.
- Disponibilidad las 24 horas del día los 7 días a la semana, durante todo el año
- La publicidad es mundial dándose más a conocer la organización.
- Facilita las negociaciones
- Se reducen los costos para enviar información y comunicaciones a clientes, proveedores, socios, etc.
- Reducción en las cadenas de distribución
- Acceso a mayor información
- Intercambio de información con otras organizaciones.

- Genera mayores ingresos.
- Proporciona nuevos medios para aumentar clientes
- Generar Nuevos modelos de negocio.
- Ofrecer nuevos servicios.
- Mayor contacto con el cliente.
- Información más detallada de los productos o servicios.

2.2.1.3 DISPOSITIVOS EMPLEADOS EN REDES DE COMUNICACIONES

Los principales dispositivos[7] que se utilizan en una red de comunicaciones son:

a) Tarjetas de Red:

Las tarjetas de red son dispositivos periféricos que van dentro de los equipos, con las cuales estos se pueden conectar a redes o a otros equipos directamente, también son llamadas NIC (Network Interfaz Card), actualmente estos dispositivos ya vienen a alojados en impresoras con el fin de ser compartidas si la intervención de ordenadores.

Para el caso de las redes de datos las tarjetas de red trabajan sobre la capa física, sirviendo de interfaz con los medios de transmisión como: cables Utp, coaxial, fibra óptica o medios inalámbricos.

Ilustración 2: Interfaces de red

Fuente: Los autores

[7] El Modelo OSI y Los Protocolos de Red, Capitulo 2, p.31.

b) Router

Los Routers o enrutadores son dispositivos de hardware que son usados para interconectar redes de computadoras, su función consiste en recibir las señales que vienen por los medios (cables, fibra, o aire), y desempaquetar hasta el punto donde se pueden encontrar la dirección de origen y la de destino para poder enviar la información, por lo general estos dispositivos hacen el desempaquetado hasta el encabezado de la capa 3 o capa de red.

El enrutador conserva una tabla de enrutamiento donde encuentra todas las posibles rutas que pueden tomar los paquetes según la interfaz por donde vengan y a donde tengan que llegar.

Ilustración 3: Routers

Fuente: Los Autores

c) *Switch:*

El Switch o conmutador es un dispositivo de capa de enlace de datos que se encarga de interconectar dos o más segmentos de red pasando datos de un segmento a otro de acuerdo a la dirección MAC de destino de las tramas en la red. Los Switches son útiles para proveer seguridad al segmento de red y mejorar el rendimiento.

Ilustración 4: Switch

Fuente: Los autores

d) *Hub*:

El Hub o concentrador es un equipo de redes que permite conectar entre si otros equipos y retransmite los paquetes que recibe desde cualquiera de ellos a todos los demás. Estos dispositivos se desenvuelven en la capa física, es decir este dispositivo solo se encarga de amplificar una señal atenuada.

Debido a las exigencias de las topologías y tecnologías de red actuales los hub´s se han vuelto en gran medida obsoletos, además porque inducen a niveles altos de colisiones y tráfico de red.

Ilustración 5: Hub

Fuente: Los autores

e) *Servidores:*

Los servidores son equipos que opera ofreciendo como su nombre lo revela servicios a los equipos o clientes que necesitan de ellos, general son la base de las empresas ya que es donde ellas obtienen y guardan su información.

La información que ellos manejan constantemente hace el recorrido por todas las capas del modelo OSI.

Existen muchos tipos de servidores, entre ellos se encuentran los servidores de archivo, impresiones, correo, fax, telefonía, web, base de datos, aplicaciones, etc.

Ilustración 6: Servidores

Fuente: Los autores

f) *Workstation:*

Las Workstation o estaciones de trabajo son dispositivos computacionales simples o en otras palabras ordenadores que funcionan como clientes de una red, y son los equipos que son utilizados generalmente por los usuarios finales, a diferencia de los servidores donde sus operarios únicos y directos son los administradores de los sistemas de información.

Ilustración 7: Computador, Host o Workstation

Fuente: Los autores

g) *Firewall:*

Los corta fuegos son dispositivos, que por prevención o mitigación de las vulnerabilidades de una red, deben ser parte de ella, su función básicamente es la de filtrar los paquetes provenientes de otras redes con el fin de hallar inconsistencia en estos.

Los firewall pueden ser físicos o lógicos, es decir, los físicos son equipos, con apariencia de módems, Routers, Switches, y los lógicos son aquellos servicios que están implícitos en los sistemas operativos. El secreto del buen funcionamiento de cualquiera de los dos tipos se encuentra en la configuración que se les dé.

Ilustración 8: Firewall Netgear

Fuente: Los autores

2.2.2 MODELO OSI

El lenguaje que utilizan los seres humanos para poder comunicarse requiere de una serie de reglas, para que esta tenga un sentido entre el emisor y el receptor, así mismo el modelo OSI actúa como un contenedor de protocolos que posibilita el entendimiento de la comunicación entre dos o más dispositivos en una red de datos.

2.2.2.1 QUE ES EL MODELO OSI

"La organización internacional para la normalización conocida más por su sigla ISO (International Organization For Standardization) la cual tiene como principal función desarrollar conjuntos de normas y modelos para asuntos que van desde hacer negocios en el mercado Internacional hasta la forma en que las compañías deben seguir los estándares técnicos para la comunicación de datos. A finales de la décadas de los setenta, la organización, empezó a desarrollar un modelo conceptual para la conexión en red al que bautizo con el nombre de Open Systems Interconnection Reference Model o Modelo de Referencia de Interconexión de sistemas abiertos, conocida comúnmente como el modelo OSI.
Este modelo se convirtió en el estándar internacional para las comunicaciones en red pues ofrece un marco conceptual que permite explicar de forma más clara la manera en que los datos se desplazaban dentro de una red.

El modelo OSI es un lineamiento funcional para tareas de comunicaciones y por consiguiente no especifica un estándar de comunicación para dichas tareas. Sin

embargo, muchos estándares y protocolos cumplen con los lineamientos del modelo OSI.

Las capas del modelo OSI describen el proceso de transmisión de los datos dentro de una red. Las dos únicas capas del modelo con las que interactúa el usuario son las capas de aplicación y física.

Este modelo presenta unas normas y mecanismos que permiten dar atención para las conexiones en red como:

- La traducción de los datos a un formato adecuado para la arquitectura de red que se utiliza
- La forma como los dispositivos de una red se comunican
- Como se debe transmitir los datos a través de la red
- Como se debe tratar los errores y resolverlos
- Como tratar el direccionamiento lógico de las aplicaciones al direccionamiento físico que maneja la red.

Como se muestra en la ilustración, las capas OSI están numeradas de abajo hacia arriba. Las funciones más básicas, como el poner los bits de datos en el cable de la red están en la parte de abajo, mientras las funciones que atienden los detalles de las aplicaciones del usuario están arriba.

En el modelo OSI el propósito de cada capa es proveer los servicios para la siguiente capa superior, resguardando la capa de los detalles de cómo los servicios son implementados realmente. Las capas son abstraídas de tal manera que cada capa cree que se está comunicando con la capa asociada en la otra

computadora, cuando realmente cada capa se comunica sólo con las capas adyacentes de la misma computadora. “[8]

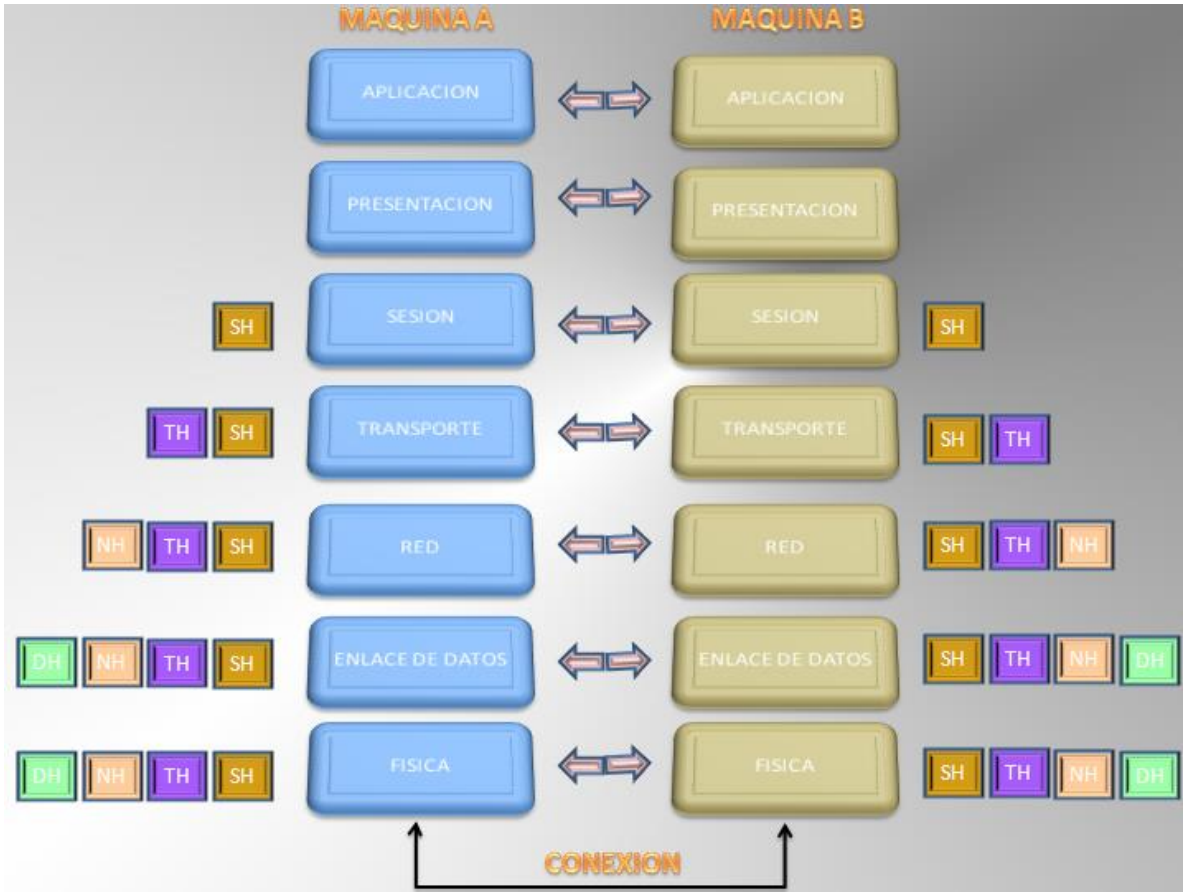
[8] MODELO OSI. [en línea]. < http://www.monografias.com/trabajos29/modelo-osi.shtml >. [Citado el 30 de Febrero de 2012].

2.2.2.2 FUNCIONAMIENTO DEL MODELO OSI

EL modelo OSI está constituido por 7 capas[9], con las cuales se efectúa el proceso de transmisión de información entre los diferentes dispositivos que hacen parte de una red de datos y cada capa se encarga de una o varias tareas específicas, quienes juntas logran el objetivo general de compartir información.

[9] BÍSARO, Mauricio y DANIZIO, Eduardo. Curso de Capacitación en Networking. Capítulo 1: Laboratorio de Redes - Diseño y Configuración de Redes de Computadoras. p. 1-7.

Ilustración 9: Cabecera Añadida por cada Capa red



Fuente: Los Autores. Tomado de : Laboratorio de redes, Ing Mauricio Bisaro, Ing Eduardo Danizio

.

Con esta figura se puede apreciar que a excepción de la capa más baja del modelo OSI, ninguna capa puede pasar información directamente a su contraparte en la otra computadora. La información que envía una computadora debe de pasar por todas las capas inferiores. La información entonces se mueve a través del cable de red hacia la computadora que recibe y hacia arriba a través de las capas de esta misma computadora hasta que llega al mismo nivel de la capa que envió la información. Al pasar por cada capa se le va a agregando un encabezado nuevo a la *PDU (Protocol Data Unit)* original hasta llegar hasta la capa física donde se convierte únicamente en bits.

Por ejemplo, si la capa de red envía información desde la computadora A, esta información se mueve hacia abajo a través de las capas de Enlace y Física del lado que envía, pasa por el cable de red, y sube por las capas Física y Enlace del lado del receptor hasta llegar a la capa de red de la computadora B.

La interacción entre las capas contiguas se denomina interface, la cual se encarga de definir los servicios que las capas inferiores ofrecen a las superiores y como son accedidos dichos servicios. Además, cada capa en una computadora actúa como si estuviera comunicándose directamente con la misma capa de la otra computadora. La serie de las reglas que se usan para la comunicación entre las capas se llama protocolo. Cada capa tiene determinados protocolos que definen la forma específica de comunicación

A continuación se verá el funcionamiento de cada capa con mayor detalle en donde se podrá apreciar más específicamente el funcionamiento del modelo OSI.

2.2.2.3 CAPA FISICA

Para lograr una comunicación[10] entre computadoras primero debe existir una *tarjeta de red* o *NIC (Network Interface Controller)* con la cual se pueda enviar y recibir las secuencias de bits que se quieren transmitir y donde van encriptados los paquetes de datos, y segundo un medio por donde viajen.

La capa física es el nivel más bajo del modelo OSI está encargada de recibir y transmitir secuencias de bits por medios, o canales de comunicación desde y

[10] CISCO SYSTEMS, CCNA Exploration 1. Capítulo 8: Capa Física del Modelo OSI. p.8.0.1 - 8.3.1

hacia la red. Es decir, que plantea los parámetros eléctricos, mecánicos, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales, ocupándose de las transmisiones a nivel de bit, por lo tanto se debe asegurar que si en esta capa se envía un bit por el medio que sea este no deberá variar en su destino.

Dentro de las tareas que desarrolla esta capa se encuentran:

- Define las características físicas (componentes y conectores mecánicos).
- Define las características eléctricas (niveles de tensión).
- Define las características funcionales de la interfaz (establecimiento, mantenimiento y liberación del enlace físico).
- Solamente reconoce bits individuales, no reconoce caracteres ni tramas multicaracter. Por ejemplo RS-232 y RS-449 que son interfaces con las que se comparten datos en series de bits.

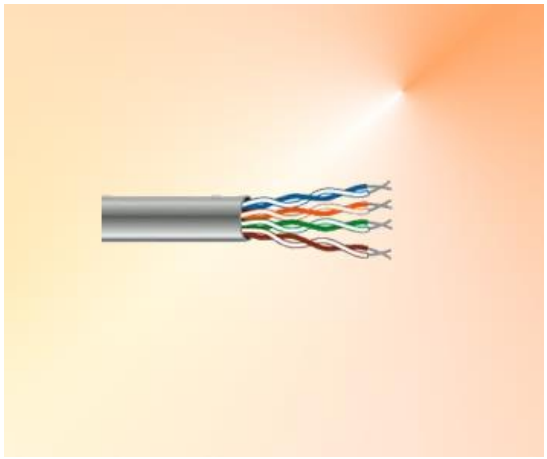
En resumidas cuentas la tarea principal que tiene esta capa es recibir una trama binaria que viene desde la capa de enlace de datos y transformarla en una señal eléctrica o electromagnética de tal forma que esta pueda ser enviada a través de la red.

Para la transmisión de las secuencias de bits en esta capa se cuenta con medios Guiados y no Guiados como los siguientes:

a) *Guiados:* Entre los medios guiados se encuentran:

Par trenzado: Es un medio físico de comunicación hecho generalmente de cobre recubierto por un material aislante, los dos cables se encuentran trenzados en forma de espiral con el fin de anular la interferencia de fuentes externas. Permiten una razón de datos de 4Mbps con un ancho de banda de 3Mhz y una distancia entre 2 y 10 kms.

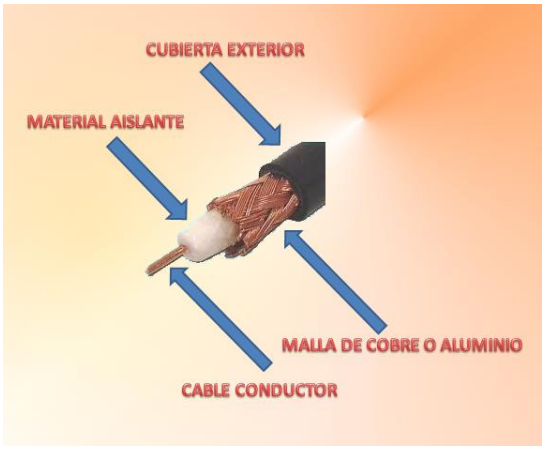
Ilustración 10: Cable utp



Fuente: Los autores

Cable coaxial: Es un medio físico generalmente cilíndrico con un alambre de cobre recubierto de un material aislante. Sobre este material se encuentra una malla de alambre que lo recubre. Constantemente es usado para transmitir señal de televisión, pero tenía una gran utilidad en sus inicios por su propiedad idónea de transmisión de voz, audio y video, además de textos e imágenes. Es poco vulnerable al ruido, permite conectar dispositivos en distancias entre 1 y 10km, una razón de datos de 500Mbps y es más común en redes de tipo BUS, Ethernet o Arcenet.

Ilustración 11: Cable Coaxial

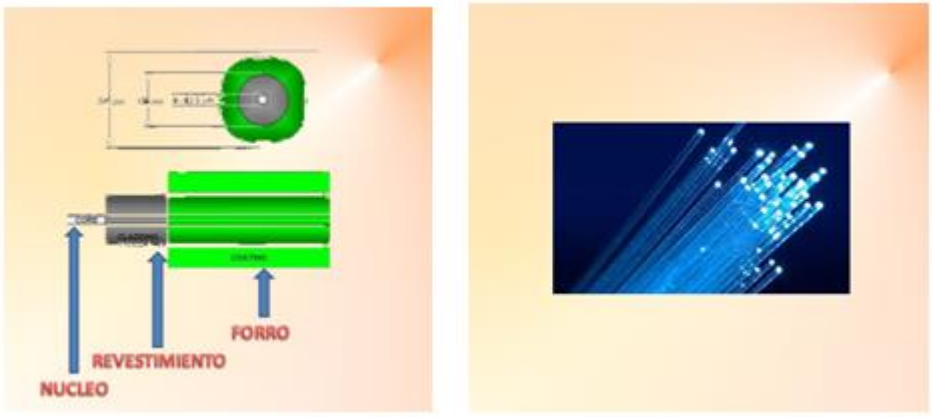


Fuente: Los autores

Fibra óptica: Es un canal que está compuesto primero que todo por una fibra de vidrio por donde viaja un haz de luz, seguido por un revestimiento, el cual está compuesto por un material con un índice de refracción menor al de la fibra óptica, de tal forma que el haz de luz se refleje por el principio de reflexión total interna hacia el núcleo. Permite que no se pierda la luz, por ultimo un recubrimiento que protege la fibra y el revestimiento de posibles amenazas del medio.

En los sistemas de comunicación se puede usar fibras Multimodo para distancias máximas de hasta 5000m o Monomodo para distancias más largas, manejando velocidades de 500Mhz/km y 100Ghz/km respectivamente.

Ilustración 12: Fibra Óptica



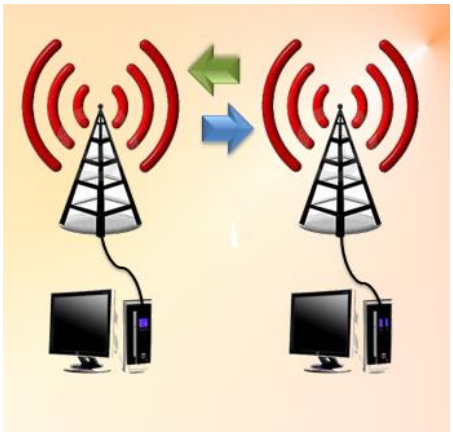
Fuente: Los autores

b) *No Guiados:*

Entre los medios no guiados se encuentran:

Radio: Las Ondas de Radio o radio enlace son un medio por el cual las secuencias de bits son enviados o recibidos a través de antenas que irradian energía electromagnética. Los datos viajan a través del aire y son recibidos desde otro punto, capaces de recorrer grandes distancias, y penetrar edificios, funciona con ondas omnidireccionales es decir las ondas se propagan en muchas direcciones, pero son vulnerables a interferencias por motores o equipos eléctricos.

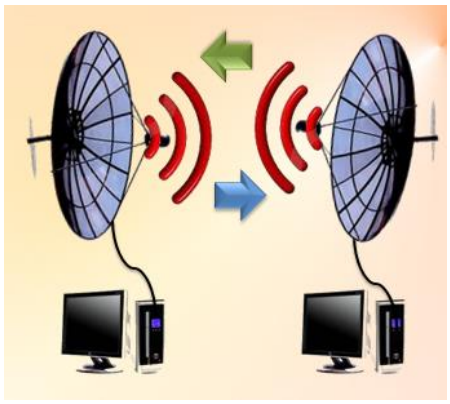
Ilustración 13: Comunicación por Radio Enlace



Fuente: Los autores

Microondas: A diferencia de las señales de radio las microondas solo viajan en una dirección, por lo que las antenas para poder transmitir información deben estar alineadas. No son buenas atravesando obstáculos, y la distancia entre antenas no debe superar 80km, pero resulta una forma económica de transferir información entre dos puntos y son más utilizadas en la transmisión de televisión y la voz.

Ilustración 14: Comunicación vía Microondas



Fuente: Los autores

Infrarrojo: Es una vía de transmisión de corto alcance con hasta 200 metros de distancia, no sirve si existen obstáculos en el medio, a diferencia de medios como (*señales de radio*) no necesitan un permiso para transmitir información.

Ondas de luz: Para lograr una comunicación exitosa con este tipo de medio de transmisión el emisor y el receptor deben estar debidamente alineados.

2.2.2.4 CAPA DE ENLACE DE DATOS

La capa de enlace de datos es la segunda capa del modelo OSI, es en la que se maneja el *direccionamiento lógico- físico* denominado de capa 2.

La función principal de ésta capa es lograr una comunicación eficiente entre dos extremos de un canal de trasmisión por medio del manejo de *tramas*.

Las principales funciones[11] de la capa de enlace de datos son las siguientes:

a) Armado y separación de tramas:

Reconocer y crear los límites de las tramas puesto que la capa física solo reconoce bytes.

b) Detección de errores:

Resuelve problemas de tramas dañadas, repetidas o perdidas. Por ejemplo, si no se recibe el acuse de recibo de una trama determinada, puede ser por que la

[11] CISCO SYSTEMS. CCNA Exploration 1. Capítulo 7: Capa de Enlace de Datos. p. 7.6.1

trama original se perdió, o porque llegó correctamente pero se perdió el acuse de recibo.

c) Control de flujo:

Al haber diferencias de rendimiento entre la maquina emisora y la receptora la capa de enlace de datos resuelve problemas de este tipo, regulando el tráfico para que no existan saturaciones o desbordes de memoria.

d) Adecuación para acceso al medio:

Se utiliza la *MAC (Medium Access Control*) la cual es una especie de subcapa que implementa protocolos para controlar el acceso al medio evitando colisiones cuando varias máquinas intentan enviar tramas al mismo tiempo.

e) Creación de Redes LAN Virtuales (VLANs):

En la Capa de Enlace de Datos se crean una serie de redes LAN lógicas que pueden abarcar varias interfaces. Es un método para crear varias redes individuales dentro de una misma red física.

f) Creación de Puertos Troncales (Trunk):

Los puertos Trunk son puertos por los cueles pasan varias redes distintas en una misma interfaz. Dichos puertos tienen acceso a todas las VLANs de forma predeterminada. Se los emplea para transmitir tráfico de múltiples VLANs a través del mismo enlace físico (generalmente empleado para conectar Switches). La encapsulación puede ser *IEEE 802.1Q* o *ISL.*

Por otro lado los principales protocolos de la capa de Enlace de Datos son los siguientes:

g) ARP (Address Resolution Protocol):

"Es un protocolo responsable de encontrar la dirección hardware (*Ethernet MAC*) que corresponde a una determinada dirección IP. Para ello se envía un paquete *(ARP request*) a la dirección de difusión de la red (broadcast MAC = FF FF FF FF FF FF) que contiene la dirección IP por la que se pregunta, y se espera a que esa máquina (u otra) responda (*ARP reply*) con la dirección Ethernet que le corresponde. Cada máquina mantiene una caché con las direcciones traducidas para reducir el retardo y la carga. ARP permite a la dirección de Internet ser independiente de la dirección Ethernet, pero esto sólo funciona si todas las máquinas lo soportan. "[12]

"La solicitud ARP se coloca en una trama *Broadcast* y se envía, todas las estaciones reciben la trama y examinan el pedido. La estación mencionada en el pedido contesta y todas las demás estaciones procesan la misma.
Las solicitudes ARP gratuitas son empleadas por dispositivos para "anunciar" su dirección IP a los demás dispositivos. Los demás dispositivos de red utilizan las solicitudes ARP gratuitas para actualizar su caché ARP. Se colocan en tramas broadcast al igual que las solicitudes ARP.

h) DTP (Dinamic Trunking Protocol):

Automatiza la configuración de los *Trunk 802.1Q/ISL*. Sincroniza el modo de Trunking en los extremos y hace innecesaria la intervención administrativa en ambos extremos. El estado de DTP en un puerto *Trunk* puede ser "*Auto", "On", "Off", "Desirable",* o *"Non-Negotiate".* Por default en la mayoría de los Switches es "Auto". " [13]

---

[12] WIKIPEDIA ORG. Address Resolution Protocol. [en línea.] < http://es.wikipedia.org/wiki/Address_Resolution_Protocol>. [Citado el 3 de Marzo de 2012].

[13] ARELLANO, Gabriel. Enterprise Security & Risk: Seguridad en Capa 2. p.11,19-23

i) *Spanning Tree Protocol (STP):*

“Es un protocolo basado en el algoritmo *Radia Perlman* que se encarga de gestionar la presencia de bucles en topologías de red cuando existen enlaces redundantes. El protocolo permite a los Switches activar o desactivar enlaces para liberar a la topología de bucles.

Como su nombre lo indica el Spanning Tree es un árbol de expansión que indica la jerarquía de Switches por los cuales deben pasar las tramas para poder evitar los bucles.

En la mayoría de redes complejas de capa 2, los Switches interconectan subredes LAN con un único Spanning Tree, el propósito de la construcción de un árbol es delegar a los Switches la tarea de descubrir de forma dinámica un subconjunto libre de bucles de la topología y al mismo tiempo que ofrezca total conectividad de capa 2 para todos los dispositivos de red.

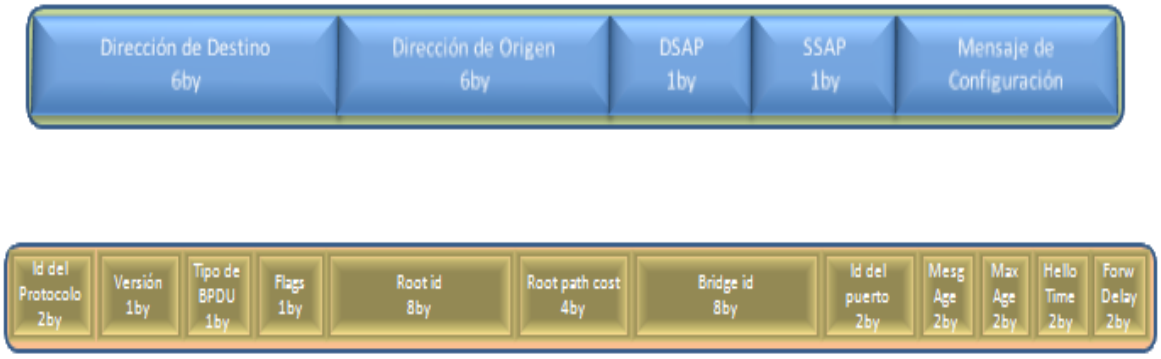
El STP posee también tolerancia a fallos al ofrecer una reconfiguración automática de la topología del árbol cuando falla un switch o una ruta sufre alguna avería.
Los Switches que conforman la topología del árbol de expansión se denominan puentes y el puente principal al que apuntan los demás se denomina puente raíz, según el protocolo cada puente debe ir identificado con un ID único que lo diferencia de los demás para poder según esa identificación elegir el nuevo puente raíz.

La elección del puente raíz se lleva a cabo por medio del intercambio de mensajes entre los bridges adyacentes, dichos mensajes se denominan Bridge Protocol

Data Unit (BPDU). La idea del intercambio de mensajes es llevar a cabo las siguientes decisiones:

- Seleccionar el puente con el ID más pequeño para que sea el único puente raíz de la LAN
- Calcular la ruta más corta desde sí mismos hasta el puente raíz.
- Para cada LAN se elige el puente con el *costo* más bajo de ruta de acceso al puente raíz, dicho puente se denomina puente designado.
- Por cada puente se debe elegir los puertos que tienen el camino más corto hasta el puente raíz, dichos puertos se denominan puertos raíz.
- De ese modo se seleccionan los puertos que se incluyen en el árbol de expansión.

Ilustración 15: Configuración de mensajes BPDU



Fuente: Los autores. Tomado de : attacks at the data link layer – Guillermo Mario Marro

En esta figura podemos observar la PDU de capa 2 (*Trama*) y la BPDU (*Bridge PDU*). A continuación se muestra el significado de cada campo:

Trama

Dirección de Destino: Dirección MAC de Destino
Dirección de Origen: Dirección MAC de Origen

BPDU

Id del Protocolo: Tipo de Protocolo utilizado.
Flags: Les indica a todos los *Bridges* que se reinicie el algoritmo del *STP.*
Root ID: Identificación del Puente raíz.
Root Path Cost: Costo de ruta hacia el Puente raíz.
Bridge ID: Identificación única del Puente.
ID del Puerto: Número de Puerto.
Hello Time: Periodicidad con la que se generan los BPDU

Normalmente después de un tiempo que el algoritmo se estabiliza, el puente raíz genera los mensajes de configuración periódicamente a cada puente de la topología y estos a su vez pasan los mensajes de configuración propios más los del puente raíz.

En caso de un cambio en la topología (un puerto o vínculo caído) el puente designado donde se produce dicho cambio genera un mensaje de cambio en la topología BPDU (Bridge Protocol Data Units) hasta llegar al puente raíz, lo que genera que se vuelva a calcular el algoritmo para asimilar los cambios y establecer de nuevo la configuración más óptima."[14]

[14] MARRO, Guillermo Mario. Attacks at the Link Layer. California, 2003. p. 12-14

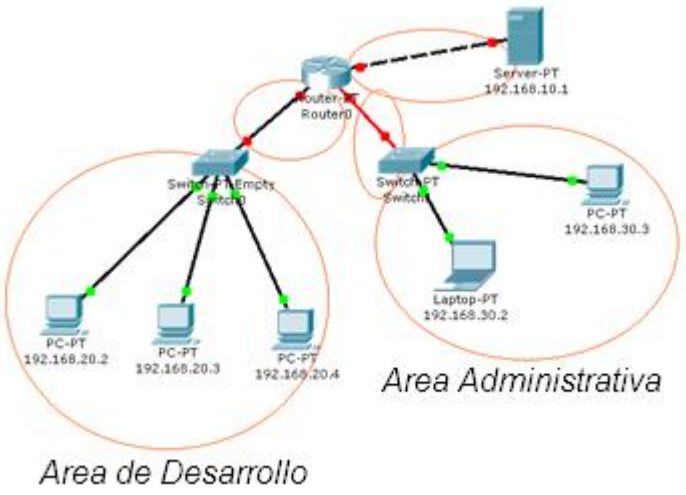
2.2.2.4 CAPA DE RED

Esta capa suministra los medios de conmutación y enrutamiento, se ocupa del control de la operación de la subred y su objetivo es hacer que los datos lleguen desde el origen a su destino mediante caminos lógicos, conocidos como circuitos virtuales, aun cuando no dispongan de una conexión directa.

La capa de red debe determinar la mejor ruta por la cual se deben enviar los datos teniendo en cuenta la velocidad y la congestión que se presenta en el recorrido de estos, del mismo modo debe disponer de las herramientas para resolver los posibles problemas de interconexión de redes heterogéneas (transmisión de protocolos diferentes por la red).

Para que los datos lleguen a su destino la capa de red cuenta con una tarea que consiste en colocarle una dirección destino y una de origen a cada paquete con el fin de que los enrutadores y host identifiquen a donde deben ser enviados.
Los administradores de red le asigna a cada dispositivo un dirección especifica de acuerdo a un plan de direccionamiento previamente establecido en la arquitectura de la red, seguidamente se podrá estructurar la topología de red en secciones o sub-redes, de acuerdo a las necesidades de los usuarios.

Ilustración 16: Subredes en una topología.



Fuente: Los autores.

La figura muestra el esquema de una topología de red, que internamente está dividida en subredes, donde cada subred representa un sector dentro de una organización, de acuerdo a como se desee la estructura de la red, se determinaran los accesos de qué equipos deben acceder a otros en una subred diferente o en su defecto, que equipos deben tener acceso a los servidores.
Como se puede observar, cada área de la empresa tiene un rango de direcciones IP específico, de tal forma que se pueda diferenciar cada sector en la organización.

El rango de direcciones de la parte administrativa corresponde a la subred 30, en la cual aplica el rango de direcciones: 192.168.30.0.

El rango de direcciones de la parte de desarrollo corresponde a la subred 20, en la cual aplica el rango de direcciones: 192.168.20.0. y sucesivamente para cada área dentro de la organización.

a) Protocolo de Internet Versión 4 (IPv4):

Es el estándar actualmente en las redes de datos para identificar dispositivos, usa direcciones de 32 bits, pero por su gran crecimiento, sumado al número de direcciones IP que se han desperdiciado ha pronosticado su salida de funcionamiento, por la alta escases de direcciones IP, favoreciendo el ingreso del protocolo de Internet versión 6 (IPv6) quien tiene por ventaja permitir más direcciones que el estándar IPv4.

En forma resumida las tareas que debe ejecutar esta capa se encuentran:

- Enrutamiento y reenvió
- El direccionamiento
- Conexión en red
- Gestión de errores
- Control de la congestión
- La secuencia de paquetes

b) ICMP (Internet Control Message Protocol):

El ICMP[15] es considerado casi una parte del protocolo IP, en consecuencia los estándares obligan que cualquier sistema que implemente protocolos IP también preste un soporte sobre ICMP. Debido a que el protocolo IP no es un protocolo 100% confiable, ahí es donde el protocolo ICMP toma su verdadera importancia, ya que se encarga de presentar los errores generados en los datagramas de los paquetes IP.

Como los protocolos ICMP serán siempre a su vez paquetes IP, se podrían presentar inconvenientes con bucles infinitos, ya que los paquetes ICMP

[15] Curso de TCP/IP: ICMP (Protocolo de Mensajes de Control de Internet). p.1-3.

comienzan a mandar errores sobre los errores de otros paquetes ICMP, pero se establece una regla donde jamás se enviara un paquete ICMP, que informe sobre errores de otro paquete ICMP.

ICMP es un mensaje comúnmente generado por los routers, o también puede ser generado por los usuarios cuando estos tratan de hacer revisiones a la red por medio de comandos como *ping* o *Traceroute*. Los mensajes se generan pero son totalmente transparentes para los usuarios, pero este tipo de protocolos pueden contener información muy relevante para los piratas informáticos.

Los Mensajes generados por el protocolo ICMP se nombran en la siguiente tabla:

Tabla 1: Errores del protocolo ICMP

Código	Descripción
0	Red Inalcanzable
1	Host Inalcanzable
2	Protocolo Inalcanzable
3	Puerto Inalcanzable
4	Paquete Demasiado grande, y no puede ser fragmentado
5	Error del router de Origen
6	Error desconocido en la red de destino
7	Error desconocido en el host de destino
8	Host de origen aislado
9	Acceso no autorizado a al red de destino
10	Acceso no autorizado al host de destino
11	La red es inalcanzable para el tipo de servicio especificado
12	El host es inalcanzable para el tipo de servicio especificado
13	Comunicación no autorizada
14	Violación de las reglas de precedencia de hosts
15	Corte de precedencia

Fuente: Los Autores. Basados en [11].

2.2.2.6 CAPA DE TRANSPORTE

Esta capa[16] se encarga de la comunicación entre los host de origen y destino, el control de flujo de una manera confiable y la detección errores. La capa de Transporte posibilita la segmentación de datos y ofrece el control requerido para unir las partes dentro de los diferentes *streams* de comunicación. Cada dato es etiquetado con un encabezado que tiene un número del puerto que identifica la aplicación de origen.

Las principales funciones de la capa de transporte son:

- Segmentación de datos y gestión de cada porción. Cada sección de datos de aplicación requiere que se agreguen encabezados en la capa de Transporte para indicar la comunicación a la cual está asociada.

- Reensamble de segmentos en flujos de datos de aplicación. Los protocolos de la capa de Transporte describen cómo se utiliza la información de encabezado de dicha capa para Reensamblar las secciones de datos en streams y enviarlas a la capa de Aplicación

- Identificación de las diferentes aplicaciones. la capa de Transporte debe identificar la aplicación de destino. Para lograr esto, la capa de Transporte asigna un identificador a la aplicación. Los protocolos denominan a este identificador número de puerto. A todos los procesos de software que requieran acceder a la red se les asigna un número de puerto exclusivo en

[16] CISCO SYSTEMS, CCNA Exploration 1. Capítulo 4: Capa de Transporte del Modelo OSI. p.4.1.1 – 4.1.5.2

ese host. Este número de puerto se utiliza en el encabezado de la capa de Transporte para indicar con qué aplicación está asociada esa sección de datos.

Cabe recordar que la función principal de la capa de Transporte es administrar los datos de aplicación para las conversaciones entre hosts. Sin embargo, las diferentes aplicaciones tienen diferentes requerimientos para sus datos y, por lo tanto, se han desarrollado diferentes protocolos de Transporte para satisfacer estos requerimientos.

Un protocolo de la capa de Transporte puede implementar un método para asegurar la entrega confiable de los datos. En términos de redes, confiabilidad significa asegurar que cada sección de datos que envía el origen llegue al destino. En la capa de Transporte, las tres operaciones básicas de confiabilidad son:

- Seguimiento de datos transmitidos.
- Acuse de recibo de los datos recibidos.
- Retransmisión de cualquier dato sin acuse de recibo.

Esto requiere que los procesos de la capa de Transporte de origen mantengan el seguimiento de todas las porciones de datos de cada conversación y retransmitan cualquiera de los datos que no dieron acuse de recibo por el destino. La capa de Transporte del host de recepción también debe rastrear los datos a medida que se reciben y reconocer la recepción de los datos.

Estos procesos de confiabilidad generan un uso adicional de los recursos de la red debido al reconocimiento, rastreo y retransmisión. Para admitir estas operaciones de confiabilidad se intercambian más datos de control entre los hosts emisores y receptores. Esta información de control está contenida en el encabezado de la Capa de transporte.

Tabla 2: Encabezados TCP y UDP

Fuente: CCNA Exploration 1 Apartado 4.1.4.1

En la figura anterior se muestra la cabecera del protocolo TCP, que consta de diez campos, el primer campo es el Puerto de origen, sesión TCP en el dispositivo que abre una conexión normalmente con un valor aleatorio superior a 1023 y un Puerto de destino que identifica el protocolo de la capa superior o la aplicación del sitio remoto, también se encuentra un Numero de secuencia (SYN) que especifica el número del ultimo octeto (byte) en el segmento y un Numero de acuse de recibo (ACK) que especifica el ultimo octeto esperando por el receptor.

La longitud del encabezado, especifica el segmento en bytes, el Checksum se utilizada para la verificación de errores en el encabezado y los datos, la Ventana muestra la cantidad de octetos que pueden enviarse antes de esperar el acuse de recibo.

El campo Urgente es utilizado únicamente con una señalización (URG). Las Opciones es información opcional y los Datos son de la capa de aplicación.
La cabecera UDP contiene 4 campos , Los campos de puerto origen y destino los cuales son de 16 bits que identifican éste proceso, continua el campo que indica el tamaño en bytes del datagrama UDP incluidos los datos y por último el campo de la cabecera restante es una suma de comprobación de 16 bits que abarca una pseudo-cabecera IP, es decir el Checksum.

La capa de transporte posee dos protocolos "TCP y UDP"[17], los cuales se definen a continuación:

a) Protocolo TCP:

TCP (Transport Control Protocol), es el empleado en la mayoría de los servicios que componen Internet actualmente. Es un protocolo fiable, es decir, se asegura de que los paquetes da datos llegan al otro extremo mediante el uso de números de secuencia y de confirmaciones de recepción (ACKs), y es orientado a conexión, es preciso que las dos partes que van a comunicarse conozcan a la otra y establezcan una conexión formal. Asimismo, está debería terminarse de forma adecuada. Por último se trata de un servicio de stream, ya que las partes intercambian flujos de datos de 8 bits (1 byte), por lo que no existen marcadores en los datos, sólo información.

b) Protocolo UDP:

UDP (User Datagram Protocol), es un protocolo muy sencillo, no orientado a conexión y no fiable, por lo que son los protocolos de nivel superior los que deben

[17] PÁEZ , Raúl, Análisis de Seguridad de la Familia de Protocolos TCP/IP y sus Servicios Asociados, 1 ed, 2002. p.23.63-93

asegurarse de la recepción de los datos. Cada operación de envío genera un único datagrama UDP. Es empleado principalmente en aplicaciones multimedia, para el envío de flujos de información sin un coste de conexión asociado.

Tabla 3: Números de Puertos

Rango de números de puerto	Grupo de puertos
De 0 a 1023	Puertos bien conocidos (Contacto)
De 1024 a 49151	Puertos registrados
De 49152 a 65535	Puertos privados y/o dinámicos

Fuente: CCNA Exploration 1 Apartado 4.1.5.2

“El puerto de origen del encabezado de un segmento se genera de manera aleatoria. Siempre y cuando no entre en conflicto con otros puertos en uso en el sistema, el cliente puede elegir cualquier número de puerto. El número de puerto actúa como dirección de retorno para la aplicación que realiza la solicitud. La capa de Transporte mantiene un seguimiento de este puerto y de la aplicación que generó la solicitud, de manera que cuando se devuelva una respuesta, pueda ser enviada a la aplicación correcta. El número de puerto de la aplicación que realiza la solicitud se utiliza como número de puerto de destino en la respuesta que vuelve del servidor.

Puertos más utilizados en los protocolos TCP y UDP en la capa de transporte.

21 (TCP/UDP) FTP
23 (TCP/UDP) Telnet
25 (TCP/UDP) SMTP
80 (TCP/UDP) HTTP - Web
110 (TCP/UDP) POP3

443 (TCP) HttpS
6891-6900 (TCP) MSN Messenger (archivos)
6901 (TCP) MSN Messenger (voz) "[18]

2.2.2.7 CAPA DE SESION

Esta capa cuenta con un protocolo de unidad de datos (PDU), lo que quiere decir que la capa de sesión cuenta con unidades de datos que se encargan de decidir si el envío de datos de una presentación a otra va a ser alternada.
Las opciones para transmisión son:
Sincronizada: Quiere decir que mientras un punto trasmite el otro escucha, hasta que se deje de trasmitir no podrá hacerlo el otro.
Asíncrona: Se envía información sin esperar nada a cambio.
La capa de sesión también actúa de agente de tráfico, ósea que cuando una máquina está transmitiendo y otras quieren transmitir, ella es la encargada de controlar cuando y como se va a establecer la transmisión.
La característica principal de la capa de sesión es de establecer, administrar y finalizar las transmisiones entre dos host que se están comunicando, restaura sesión, sincroniza la transmisión entre las capas, dispone de la transferencia, controla el flujo y permite que varios usuarios puedan establecer una conversación al tiempo.

[18] CISCO SYSTEMS, CCNA Exploration 1. Capítulo 4: Capa de Transporte del Modelo OSI. p.4.1.1 – 4.1.5.2

Ilustración 17: La comunicación en la capa de sesión

Fuente: Los Autores. Basados en La Pila OSI y los Protocolos de Red, Página 7.

Como se puede ver en la Ilustración 17, un host o estación de trabajo hace una petición de algún servicio al servidor, cuando el servidor responde se establece una sesión entre ellos.

2.2.2.8 CAPA DE PRESENTACIÓN

"El nivel de presentación se encarga de conseguir que las diferentes plataformas (sistemas operativos, procesadores, etc.) se puedan entender al conectarse por medio de una misma red. Dicho de otra manera, soluciona el problema de la heterogeneidad definiendo una manera universal de codificar la información. Dicha

codificación puede tener propiedades de eficiencia (por medio de la compresión, por ejemplo), propiedades de confidencialidad (por medio de la criptografía), etc."[19]

La capa de presentación facilita el trabajo de las entidades de la capa de aplicación, de las diferentes sintaxis abstractas o de transferencia, así también como de la semántica de los datos intercambiados. Sus servicios incluyen:

• Conversiones de código y de formatos de datos.
• La compresión y la encriptación de los datos.

Un ejemplo, es la codificación de datos en una forma estándar acordada. La información en una computadora se representa como cadena de caracteres, enteros, cantidades de punto flotante; estos códigos se representan con cadenas de caracteres como (ASCII, Unicode) y enteros (Complemento a uno o a dos). Con el fin de comunicar computadores con representaciones diferentes, la información a intercambiar se puede definir en forma abstracta, junto con un código estándar que se use en el cable. De esta manera, la capa presentación adapta la representación que se usa dentro de cada computadora, a la representación estándar de la red y viceversa.

[19] BARCELÓ ORDINAS, José María; ÍÑIGO GRIERA; MARTÍ ESCALÉ, Ramón; PEIG OLIVÉ, Enric; PERRAMON TORNIL, Xavier. Redes de Computadores. Barcelona: 1 ed, 2004. p.47

2.2.2.9 CAPA DE APLICACIÓN

La capa de aplicación permite la comunicación humana con la red de datos. Cuando se abre un explorador web, una ventana de mensajería instantánea, o se ejecuta una aplicación, existen formas de procesos o programas de software que proporcionan acceso a la red en formas de aplicaciones o servicios. Dichas formas de procesos o programas están ligadas a la capa de aplicación.

a) Aplicaciones reconocidas por la red:

Aplicaciones son los programas de software que utiliza la gente para comunicarse a través de la red. Algunas aplicaciones de usuario final son compatibles con la red, lo cual significa que implementan los protocolos de la capa de aplicación y pueden comunicarse directamente con las capas inferiores del *stack* de protocolos. Los clientes de correo electrónico y los exploradores Web son ejemplos de este tipo de aplicaciones.

b) Aplicaciones y protocolos de la capa de aplicación:

La capa de Aplicación utiliza los protocolos implementados dentro de las aplicaciones y servicios. Mientras que las aplicaciones proporcionan a las personas una forma de crear mensajes y los servicios de la capa de aplicación establecen una interfaz con la red, los protocolos proporcionan las reglas y los formatos que regulan el tratamiento de los datos. Un único programa ejecutable debe utilizar los tres componentes e inclusive el mismo nombre. Por ejemplo: cuando analizamos "Telnet" nos podemos referir a la aplicación, el servicio o el protocolo.

En el modelo OSI, se considera que las aplicaciones que interactúan directamente con las personas se encuentran en la parte superior del stack, al igual que las personas. Al igual que todas las personas dentro del modelo OSI, la capa de Aplicación se basa en las funciones de las capas inferiores para completar el proceso de comunicación. Dentro de la capa de aplicación, los protocolos especifican qué mensajes se intercambian entre los host de origen y de destino, la sintaxis de los comandos de control, el tipo y formato de los datos que se transmiten y los métodos adecuados para notificación y recuperación de errores.

c) *Protocolos de la Capa de Aplicación:*

Los protocolos de la capa de aplicación son utilizados tanto por los dispositivos de origen como de destino durante una sesión de comunicación. Para que las comunicaciones sean exitosas, deben coincidir los protocolos de capa de aplicación implementados en el host de origen y destino.

Los protocolos establecen reglas consistentes para intercambiar datos entre las aplicaciones y los servicios cargados en los dispositivos participantes. Los protocolos especifican cómo se estructuran los datos dentro de los mensajes y los tipos de mensajes que se envían entre origen y destino. Estos mensajes pueden ser solicitudes de servicios, acuses de recibo, mensajes de datos, mensajes de estado o mensajes de error. Los protocolos también definen los diálogos de mensajes, asegurando que un mensaje enviado encuentre la respuesta esperada y se invoquen los servicios correspondientes cuando se realiza la transferencia de datos.

Muchos y diversos tipos de aplicaciones se comunican a través de las redes de datos. Por lo tanto, los servicios de la capa de Aplicación deben implementar protocolos múltiples para proporcionar la variedad deseada de experiencias de

comunicación. Cada protocolo tiene un fin específico y contiene las características requeridas para cumplir con dicho propósito. Deben seguirse los detalles del protocolo correspondiente a cada capa, así las funciones en una capa se comunican correctamente con los servicios en la capa inferior.
Los protocolos de la capa de aplicación cumplen las siguientes funciones definiendo:

- los procesos en cada uno de los extremos de la comunicación
- los tipos de los mensajes
- la sintaxis de los mensajes
- el significado de los campos de información
- la forma en que se envían los mensajes y la respuesta esperada.
- la interacción con la próxima capa inferior.

Los principales protocolos son:

"HTTP (Hipertext Transfer Protocol): Cuando se escribe una dirección Web (o URL) en un explorador de Internet, el explorador establece una conexión con el servicio Web del servidor que utiliza el protocolo HTTP. URL *(Localizador Uniforme de Recursos)* y URI *(Identificador Uniforme de Recursos)* son los nombres que la mayoría de las personas asocian con las direcciones Web.

El URL http://www.cisco.com/index.html es un ejemplo de un URL que se refiere a un recurso específico: una página Web denominada index.html en un servidor identificado como cisco.com

DNS (Domain Name Systems): En redes de datos, los dispositivos son rotulados con direcciones IP numéricas para que puedan participar en el envío y recepción de mensajes a través de la red, esto resulta molesto para las personas y por eso los nombres de dominio fueron creados para convertir las direcciones numéricas en nombres simples y reconocibles.

En Internet, esos nombres de dominio, como www.cisco.com, son mucho más sencillos de recordar que 198.133.219.25, que es la dirección numérica real para este servidor. Además, si Cisco decide cambiar la dirección numérica, para el usuario es transparente ya que el nombre de dominio seguirá siendo www.cisco.com. La nueva dirección simplemente estará enlazada con el nombre de dominio existente y la conectividad se mantendrá.

El *Sistema de nombres de dominio* (DNS) se creó para que el nombre del dominio busque soluciones para estas redes. DNS utiliza un conjunto distribuido de servidores para resolver los nombres asociados con estas direcciones numéricas.

El protocolo DNS define un servicio automatizado que coincide con nombres de recursos que tienen la dirección de red numérica solicitada. Incluye las consultas sobre formato, las respuestas y los formatos de datos.

SMB (Server Message Block): El Bloque de mensajes del servidor (SMB) es un protocolo cliente-servidor para compartir archivos. IBM desarrolló el Bloque de mensajes del servidor (SMB) a fines de la década del '80 para describir la estructura de recursos de red compartidos, como directorios, archivos, impresoras y puertos seriales. Es un protocolo de solicitud-respuesta. A diferencia del protocolo para compartir archivos respaldado por FTP, los clientes establecen una conexión a largo plazo con los servidores. Una vez establecida la conexión, el usuario del cliente puede acceder a los recursos en el servidor como si el recurso fuera local para el host del cliente.

DHCP (Dynamic Host Configuration Protocol): El servicio Protocolo de configuración dinámica de host (DHCP) permite a los dispositivos de una red obtener direcciones IP y demás información de un servidor DHCP. Este servicio automatiza la asignación de direcciones IP, máscaras de subred, *Gateways* y otros parámetros de redes IP.

DHCP permite a un host obtener una dirección IP en forma dinámica cuando se conecta a la red. Se realiza el contacto con el servidor de DHCP y se solicita una dirección. El servidor DHCP elige una dirección de un rango configurado de direcciones denominado "pool" y se la asigna ("alquila") al host por un período establecido.

En redes locales más grandes o donde cambia frecuentemente la población usuaria, es preferible el DHCP. Los nuevos usuarios llegan con computadoras portátiles y necesitan una conexión. Otros tienen nuevas estaciones de trabajo que necesitan conexión. En lugar de tener direcciones IP asignadas por el administrador de red en cada estación de trabajo, resulta más eficiente tener direcciones IP asignadas en forma automática utilizando un DHCP.

SMTP (Simple Mail Transfer Protocol) / POP (Post Office Protocol): E-mail, el servidor de red más conocido, ha revolucionado la de comunicarse del ser humano, por su simpleza y velocidad. Inclusive para ejecutarse en una computadora o en otro dispositivo, los e-mails requieren de diversos servicios y aplicaciones. Dos ejemplos de protocolos de capa de aplicación son *Protocolo de oficina de correos (POP)* y *Protocolo simple de transferencia de correo (SMTP).* Como con HTTP, estos protocolos definen procesos cliente-servidor.

Cuando una persona escribe mensajes de correo electrónico, generalmente utiliza una aplicación denominada *Agente de usuario de correo (MUA)* o cliente de correo electrónico. MUA permite enviar los mensajes y colocar los mensajes recibidos en el buzón del cliente; ambos procesos son diferentes.

Para recibir e-mails desde un servidor de e-mail, el cliente de correo electrónico puede utilizar un POP. Al enviar un e-mail desde un cliente o un servidor, se utilizan formatos de mensajes y cadenas de comando definidas por el protocolo SMTP. En general, un cliente de correo electrónico proporciona la funcionalidad de ambos protocolos dentro de una aplicación.

Telnet: Telnet se remonta a principios de la década de los setenta y se encuentra entre los servicios y protocolos de capa de aplicación más antiguo. Telnet proporciona un método estándar de emulación de dispositivos de terminal basados en texto en la red de datos. El protocolo y el software del cliente que implementa el protocolo comúnmente se definen como Telnet. Y como consecuencia, una conexión que utiliza Telnet se llama Sesión o *conexión de terminal virtual (VTY).* En lugar de utilizar un dispositivo físico para conectar al servidor, Telnet utiliza software para crear un dispositivo virtual que proporciona las mismas funciones que una sesión terminal con acceso a la *Interfaz de línea de comandos (CLI)* del servidor." [20]

[20] CISCO SYSTEMS, CCNA Exploration 1. Capítulo 3: Protocolos y Funcionalidad de la Capa de Aplicación. p.3.1.2

SEGURIDAD

3.1 SEGURIDAD EN LAS ORGANIZACIONES

La seguridad en las redes se refiere a la protección de la información, mediante políticas de seguridad, que logran disminuir las vulnerabilidades en las redes. Tres aspectos como la confidencialidad la integridad y la disponibilidad se convierten en los objetivos que los intrusos intentaran atacar.

a) Confidencialidad:

La confidencialidad hace referencia a los datos que viajan a través de las redes, que solo deben llegar a manos del usuario con su debido permiso. Un ejemplo claro se podría observar en el robo de contraseñas donde personas indeseadas al poseerlas pueden llegar a obtener información de forma ilícita.

b) Integridad:

Mantener la integridad de la información es vital, debido a que ésta debe llegar a su destino de la misma forma que salió del origen, es decir que en el recorrido los bits que la integran no sufran alguna alteración.

c) Disponibilidad:

Otra característica importante de la información, es que cuando una persona necesite de ésta, pueda tener acceso a ella en cualquier instante. Los atacantes muchas veces van a intentar atentar contra la disponibilidad de la información, inundando las redes con datos irrelevantes ocasionando así mismo la caída de servidores.

3.1.1 ANATOMÍA DE UN ATAQUE INFORMÁTICO

3.1.1.1 RECONOCIMIENTO

En la etapa de reconocimiento se estudia a la posible víctima, por medio de diferentes técnicas que proporcionen la información necesaria para un posible ataque.

3.1.1.2 EXPLORACIÓN

La información obtenida anteriormente es utilizada para lograr datos más relevantes como la dirección IP, contraseñas, host entre otros.

3.1.1.3 OBTENER EL ACCESO

Ahora se analiza las debilidades del sistema, permitiendo así una elaboración inicial del ataque, ataque de los cuales se hablara más adelante en este documento.

3.1.1.4 MANTENER EL ACCESO

Como ya se ha logrado el ataque, los usuarios maliciosos pretenderán mantener el acceso permanente para cuando lo deseen utilizar, usando herramientas como puertas traseras, gusanos, etc.

3.1.1.5 BORRAR HUELLAS

Habiendo logrado los objetivos que se ha propuesto el atacante, buscara la manera de no ser detectado borrando cualquier rastro de lo que haya hecho.

Ilustración 18: Anatomía de un ataque informático

Fuente: Los Autores.

3.1.2 LA IMPORTANCIA DE LOS DATOS EN LAS ORGANIZACIONES

Basados en [1], determinar el valor de los datos es algo relativo, pues la información muchas veces no es un recurso al que se le dé la importancia que requiere debido a su intangibilidad. Todo lo contrario sucede con los equipos, la documentación o las aplicaciones.

Cuando se habla del valor de la información se hacer referencia por ejemplo a que tan peligroso resulta enviar información de una tarjeta de crédito a través de internet para hacer una compra, en una red gigantesca donde viajan no solo 16 dígitos de la tarjeta sino millones de datos más, gráficas, voz y video.

El peligro radica en el momento en el cuál la información de la tarjeta, unida a la de miles de clientes más, reposa en una base de datos de la compañía con la que se efectuó el negocio. Si se realizase un acceso no autorizado a esta base de datos, es posible que un tercero tenga acceso a los datos y tarjetas de todos los clientes de la compañía.

Para llevar esto a datos reales, se puede tomar como base el reporte de la agencia norteamericana Defense Information Systems Agency titulado "*Defending The Defense Information Infraestructure – Defense Information Systems Agency*" del 9 de julio de 1996, en donde se muestra que las corporaciones más grandes

de los Estados Unidos reportaron pérdidas estimadas en US$ 800 millones debido a ataques a sus infraestructuras de red.

También cabe resaltar el informe de marzo de 1997 de la organización The *Computer Security Institute (CSI)* en donde se muestra que el crimen de cómputo continuaba en alza y se habían reportado pérdidas superiores a los US$ 100 millones solo el primer cuarto de ese año.

Aunque puede parecer datos antiguos, dan a conocer una tendencia a los ataques informáticos y conlleva a pensar en las nuevas y sofisticadas técnicas que hoy en día poseen los hackers para llevar a cabo toda clase de infiltraciones y ataques a las redes de las organizaciones.

3.1.3 POLITICAS DE SEGURIDAD INFORMÁTICA (PSI) Y SU IMPACTO EN LA ORGANIZACIÓN

Las políticas de seguridad [1] informática establece la manera como debe reaccionar el personal en relación con los recursos y servicios informáticos de importancia en la organización. En ella se hace una descripción de los elementos informáticos que se desean proteger y el porqué de ello.

Las PSI requieren de la disposición de todos y cada uno de los integrantes de la organización para lograr a un acuerdo de lo que se considera importante permitiendo la eficiencia de su implementación.

Para llevar a cabo un conjunto de políticas de seguridad informática se debe tener en cuenta los siguientes aspectos:

- Alcance de las políticas, en donde se invita a todo el personal a darle a la información la importancia que merece como uno de los principales activos para el correcto desarrollo de los procesos empresariales.
- Objetivos de la política donde se describa claramente los elementos involucrados.
- Responsabilidades por cada servicio y recurso informático de la organización.
- Requerimientos necesarios en las configuraciones que apliquen al alcance de la política de seguridad.
- Se definen las violaciones a la política y las consecuencias de esto.
- Asignación de responsabilidades a los usuarios de acuerdo a la información que tienen acceso.

Con las políticas de seguridad informática (PSI) bien definidas en una organización, se posee un estándar de acción comunal a la hora de presentarse fallas y/o ataques en los sistemas de información, lo que permite que todos los entes de la organización contribuyan en un mismo rumbo hacia una posible mitigación o solución.

3.1.4 VULNERABILIDADES EN LAS ORGANIZACIONES

Las organizaciones modernas están sujetas a una serie de vulnerabilidades internas y externas, que las hacen presa fácil de los ataques por parte de actores malintencionados provocándoles así fallas a sus sistemas de información. A continuación se muestra una breve historia de las vulnerabilidades que poseen las empresas y como han ido evolucionando a través del tiempo.

3.1.4.1 HISTORIA DE LAS VULNERABILIDADES

En los primeros años [20], los ataques involucraban poca sofisticación técnica. Los ataques internos se basaban en utilizar los permisos para alterar la información. Los externos se basaban en acceder a la red simplemente averiguando una clave válida.

A través de los años se han desarrollado formas cada vez más sofisticadas de ataque para explotar vulnerabilidades en el diseño, configuración y operación de los sistemas, esto permitió a los nuevos atacantes tomar control de sistemas completos, produciendo verdaderos desastres, que en muchos casos llevaron a la desaparición de aquellas organizaciones (en su mayoría fueron empresas que poseían altísimo grado de dependencia tecnológica, como bancos, servicios automáticos, etc).

Estos nuevos métodos de ataque han sido automatizados, por lo que en muchos casos sólo se necesita un conocimiento técnico básico para realizarlos.
Bruce Scheiner ha clasificado las generaciones de ataques en la red existentes a lo largo del tiempo. A continuación se aprecia dicha clasificación:

a) *La primera generación: Ataque Físico*

Ataques que se centraban en los componentes electrónicos como ordenadores, dispositivos y cables.

b) *La segunda generación: Ataque Sintáctico*

Las pasadas décadas se han caracterizado por ataques contra la lógica operativa de los ordenadores y las redes, es decir, pretendían explotar las vulnerabilidades

de los programas, de los algoritmos de cifrado y de los protocolos, así como permitir la denegación del servicio prestado.

c) *La tercera generación: Ataque Semántico*

Se basan en la manera en que los humanos asocian significado a un contenido. El inicio de este tipo de ataques surgió con la colocación de información falsa en boletines informativos o e-mails, por ejemplo, para beneficiarse de las inversiones dentro de la bolsa financiera. También pueden llevarse a cabo modificando información caduca.

Esta generación de ataques se lleva a su extremo si se modifica el contenido de los datos de los programas, que son incapaces de sospechar de su veracidad, como por ejemplo la manipulación del sistema de control de tráfico aéreo, el control de un coche inteligente, la base de datos de los libros más vendidos o de índices bursátiles como el NASDAQ.

3.1.4.2 DEBILIDADES EN LAS ORGANIZACIONES

A continuación se muestra un recuento de las debilidades que son más comúnmente explotadas en las organizaciones y que conllevan a la generación de vulnerabilidades hacia los ataques informáticos:

a) *Ingeniería Social*

La ingeniería social es una debilidad enfocada a encontrar las falencias del factor humano en una organización, los atacantes saben cómo aprovechar dichas falencias para realizar sus actos delictivos.

En la ingeniería social, los seres humanos representan un talón de Aquiles a la hora de buscar la manera de tener acceso a la información de una organización, puesto que a diferencia de los componentes electrónicos son un elemento manipulable capaz de romper las reglas establecidas en las políticas de seguridad de la información.

Los atacantes se aprovechan del desconocimiento, negligencia o ignorancia de las personas para acceder a la información o generar el ataque en los sistemas informáticos de las organizaciones.

b) Factor Insiders

Los *Factor Insiders* son agentes dentro del interior de una organización que se encargan de atacar sistemas informáticos. Comúnmente dichos agentes son los mismos empleados que posiblemente pueden estar dentro de la organización única y exclusivamente con la intención de hacer estragos. Por otro lado también pueden ser empleados que debido a un disgusto, problema o conflicto con los demás, han decidido a manera de venganza hacer algún tipo de acto delictivo.
Los *Factor Insiders* por su naturaleza de actuar dentro de la organización, son en gran medida inmunes a los sistemas de seguridad estándar que se aplican en las empresas, pues éstos van enfocados hacia el exterior.

c) Códigos Maliciosos

Los códigos maliciosos o *Malware* son programas que causan algún tipo de daño en el sistema informático. Los tipos de *Malware* más comúnmente conocidos son los troyanos, gusanos, virus informáticos, spyware, BackDoors, rootkits, Keyloggers, entre otros.

El tipo de código malicioso más utilizado es el troyano, según *el Informe sobre malware en América Latina, de ESET Latinoamérica*, representa el 80% de los ataques informáticos reportados en el estudio.

Los troyanos son una aplicación común que ingresa al sistema de forma sigilosa y activan una carga maligna denominada *Payload* que contiene el código con las instrucciones dañinas. Dicho código puede contener instrucciones para dañar el disco duro, eliminar archivos, monitorear el tráfico de red, contar el número de clics, el número de pulsaciones en el teclado entre otras.

Junto con los troyanos, los atacantes pueden agregar otra clase de intrusiones que aprovechan la brecha abierta que ha dejado ya el troyano. Ataques como *rootkits* para borrar las huellas que han dejado en el sistema y así poder seguir efectuando nuevas intrusiones sin ser descubiertos.

d) Contraseñas

Las contraseñas [17] representan un elemento de seguridad clave para los atacantes o intrusos, pues la mayoría de sistemas informáticos requieren de una autenticación a los usuarios por medio de contraseñas. El uso de contraseñas para mantener la confidencialidad y la seguridad de los diferentes usuarios en la red, es una práctica de seguridad antigua pero aún hoy en día se mantiene vigente por su efectividad.

La fortaleza de la contraseña se enfoca en que sea un código difícil de descifrar, que se mantenga en secreto. Sin embargo esto hace que sea vulnerables a técnicas de ingeniería social.

"De nada sirve utilizar contraseñas fuertes si luego son olvidadas o compartidas, ya que con ello se compromete la seguridad de todo el mecanismo de autenticación"[21]

e) *Configuraciones Predeterminadas*

Las configuraciones predeterminadas son un factor de fácil vulneración por parte de los intrusos y atacantes, puesto que los códigos maliciosos e intrusiones, son hechos pensando inicialmente en que el equipo o sistema a atacar se encuentra configurado de forma predeterminada. De esta forma el intruso puede sacar provecho del hecho de saber los parámetros y estándares que conforman dicha configuración.

El *Exploit* es un tipo de código que se encarga precisamente en aprovechar las configuraciones predeterminadas de un equipo. También existen sitios web que contienen bases de datos con toda la información de usuarios, contraseñas, códigos de acceso, valores por defecto de los sistemas operativos, entre otros.

f) *OSINT (Open Source Intelligent)*

La *OSINT (Open Source Intelligent)* es la manera como los atacantes o intrusos obtienen la información de los sistemas a atacar, haciéndolo en fuentes abiertas (públicas).

La información recolectada por el atacante es una consecuencia de una investigación rigurosa sobre el objetivo basada en recursos públicos. Los

[21] MIERES, Jorge. Ataques Informáticos: Debilidades de Seguridad Comúnmente Explotadas, 2009. p. 8-15.

atacantes gastan más del 70% del tiempo en la preparación previa antes del ataque, para cuando llegue el momento les sea mucho más fácil.

Los principales mecanismos para la obtención de información son el *Reconnaissance, Discovey, Footprinting, Google Hacking*.

3.2 SEGURIDAD EN EL MODELO OSI

Una vez vistas las principales vulnerabilidades y debilidades que aplican a las organizaciones, es importante enfocar este subcapítulo a las vulnerabilidades y ataques al modelo OSI propiamente.

3.2.1 VULNERABILIDADES EN EL MODELO OSI

El modelo OSI está sujeto a varias vulnerabilidades [20] , a continuación se describen las vulnerabilidades que afectan a todo el modelo y posteriormente a cada una de las capas que lo conforman:

3.2.1.1 VULNERABILIDADES GENÉRICAS

Las vulnerabilidades pretenden describir las debilidades y los métodos más comunes que se utilizan para perpetrar ataques a la seguridad de la familia de protocolos TCP/IP (confidencialidad, integridad y disponibilidad de la información). Los ataques pueden estar motivados por diversos objetivos, incluyendo fraude, extorsión, robo de información confidencial, venganza, acceso no autorizado a un sistema, anulación de un servicio o simplemente el desafío de penetrar un sistema.

Éstos pueden provenir principalmente de dos fuentes:

- Usuarios autentificados, al menos a parte de la red, como por ejemplo empleados internos o colaboradores externos con acceso a sistemas dentro de la red de la empresa. También denominados *Insiders*.

- Atacantes externos a la ubicación física de la organización, accediendo remotamente. También denominados *outsiders*

Las vulnerabilidades pueden clasificarse según dos criterios:

Criterio 1 : Número de paquetes a emplear en el ataque:

- Atomic: se requiere un único paquete para llevarla a cabo.
- Composite: son necesarios múltiples paquetes.

Criterio 2: Información necesaria para llevar a cabo el ataque:

- Context: se requiere únicamente información de la cabecera del protocolo.
- Content: es necesario también el campo de datos o *Payload*.

Tabla 4: División de vulnerabilidades

	Atomic	**Composite**
Context	*Ping of death* *Land attack* *WinNuke*	*Port scan* *SYN Flood* *TCP hijacking*
Content	*DNS attack* *Proxied RPC* *IIS attack*	*SMTP attacks* *String matches* *Sniffing*

Fuente: PÁEZ SILES, RAÚL Análisis de Seguridad de la Familia de Protocolos tcp-ip y sus Servicios Asociados, pagina 26

Imagen. División de vulnerabilidades según criterios.

A continuación se muestra los ataques y vulnerabilidades a las cuales están sujetas las capas del modelo OSI:

3.2.1.2 ATAQUES A LA CAPA DE APLICACIÓN

Los ataques a la capa de aplicación [20] van enfocados hacia la denegación de servicios (DoS), Códigos Maliciosos y OSINT (Open Source Intelligent) y muchos otros, los cuales veremos a continuación:

a) DNS Spoofing:

Suplantación de identidad por nombre de dominio. Se trata del falseamiento de una relación "Nombre de dominio-IP" ante una consulta de resolución de nombre, es decir, resolver con una dirección IP falsa un cierto nombre DNS o viceversa.

b) Sniffing:

Un ataque realmente efectivo, ya que permite la obtención de gran cantidad de información sensible enviada sin encriptar, como por ejemplo usuarios, direcciones de e-mail, claves, números de tarjetas de crédito. El Sniffing consiste en emplear Sniffers u olfateadores en entornos de red basados en difusión, como por ejemplo Ethernet (mediante el uso de concentradores o Hubs). El análisis de la información

trasmitida permite a su vez extraer relaciones y topologías de las redes y organizaciones.

Los Sniffers operan activando una de las interfaces de red del sistema en modo promiscuo. En este modo de configuración, el Sniffers almacenará en un log todo el tráfico que circule por la tarjeta de red, ya sea destinado o generado por el propio sistema o desde/hacia cualquiera de los sistemas existentes en el entorno de red compartido (segmento Ethernet). Asimismo, pueden ser instalados tanto en sistemas como en dispositivos de red.

La efectividad de esta técnica se basa en tener acceso (habitualmente es necesario además disponer de dicho acceso como administrador o root) a un sistema interno de la red; por tanto, no puede ser llevado a cabo desde el exterior. Antes de la instalación de un Sniffers, normalmente se instalarán versiones modificadas (*Trojanos*) de comandos como "*ps*" o "*netstat*" en entornos (Unix) para evitar que las tareas ejecutadas en el Sniffers sean descubiertas.

c) Eavesdropping:

El Eavesdropping es una variante del Sniffing caracterizada porque únicamente contempla la adquisición o intercepción del tráfico que circula por la red de forma pasiva, es decir, sin modificar el contenido de la misma.

d) Snooping:

Es otra variante dentro del Sniffing basada en el almacenamiento de la información obtenida en el ordenador del atacante (*Downloading).* También se asocia a la obtención de la información extraída de un sistema y no solo en el tráfico de red.

e) SMTP Spoofing y Spamming:

En un nivel superior, concretamente a nivel de aplicación, en el protocolo SMTP (puerto TCP 25) es posible falsear la dirección fuente de un correo o e-mail, enviando por tanto mensajes en nombre de otra persona. Es así porque el protocolo no lleva a cabo ningún mecanismo de autenticación cuando se realiza la conexión TCP al puerto asociado.

f) DoS (Denial of Servicies):

En los protocolos de los modelos TCP/IP y OSI, se analizan los ataques basados en la denegación de servicio (DoS) desde el exterior de un sistema, a través de la red, y no una vez se disponga de acceso de administrador en el mismo.
En este segundo caso, en los sistemas Unix sería tan sencillo efectuar un ataque de este tipo como eliminar todos los ficheros del sistema mediante el comando "*rm -rf / &",* haciendo depender el establecimiento del servicio por la política de backup del sistema.

Si se tiene acceso a los dispositivos de red, éstos pueden re arrancarse o apagarse, con la implicación que tendría en las comunicaciones de la red de la organización afectada. Un ataque de denegación de servicio se centra en sobrepasar los límites de recursos establecidos para un servicio determinado, obteniendo como resultado la eliminación temporal del servicio. Por ejemplo, si un servidor es capaz de procesar 10 peticiones por segundo, y se le envían 30, parte del tráfico legítimo no recibirá servicio, o incluso, puede que la saturación del tráfico provoque que el servidor deje de responder a ninguna petición.

Los destinos de estos ataques suelen ser objetivos visibles, como servidores Web, o DNS, o elementos básicos de la red, Routers o enlaces de red. Este tipo de ataques no supone ningún peligro para la seguridad de las máquinas, ya que no modifica los contenidos de la información, ni permite obtener información sensible. Simplemente persiguen entorpecer el acceso de los usuarios a los servicios de un sistema. Normalmente, una vez que el ataque finaliza, se vuelve a la situación normal. En algunas ocasiones se han empleado para encubrir otros ataques simultáneos cuyo objetivo sí era comprometer el sistema.

Asimismo, la probabilidad de que el administrador, intentando defenderse del DoS cometa un error de configuración es mayor en el momento del ataque, pudiendo dejar al descubierto una vulnerabilidad protegida previamente.

Los ataques y herramientas más empleados en estos años para llevar a cabo ataques DoS y DDoS, son:

- *Smurf,*
- *Fraggle,*
- *Trinoo,*
- *TFN,*
- *Stacheldraht,*
- *TFN2K,*
- *Mstream,*
- *T0rnkit,*
- *Trinity*
- *DDoS,*
- *Erkms,*
- *Li0n,*
- *Carko,*
- *W0rmkit.*

Así como algunos virus y/o gusanos:

- *VBS/LoveLetter,*
- *Ramen worm,*
- *VBS/OnTheFly,*
- *Cheese worm,*
- *Sadmin/IIS worm, W32/Sircam,*
- *Leaves,*
- *CodeRed,*
- *CodeRed II,*
- *Knight/Kaiten,*
- *Nimda*

g) SMTP Flood:

Mediante el envío masivo de mensajes de correo electrónico a grandes listas de usuarios de forma continua, se provoca la saturación de los servidores de correo destino o intermedios.

h) DDoS:

Una variante más potente a la de los ataques de Denegación de Servicio, son los DDoS, o ataques de denegación de servicio distribuidos, que se basan en realizar ataques DoS de forma masiva a un mismo objetivo desde diferentes localizaciones en la red, de forma que la potencia de ataque sea mucho mayor.
Si un ataque desde una fuente es potente, desde 1000 lo será mucho más, es decir, es la aplicación del “divide y vencerás” a la técnica DoS. Su origen se remonta a los comienzos de la seguridad en Internet, cuando el famoso Gusano de *Robert Morris, Jr*, desencadenó una denegación de servicio por un error de

programación. El gusano fue capaz de colapsar por aquel entonces gran parte de los sistemas existentes en Internet.

Sin embargo su expansión se ha producido principalmente en el año 2000, haciéndose eco los medios de comunicación, al surgir numerosas herramientas que permiten su ejecución, de forma coordinada y a gran escala. Un único atacante puede desencadenar una agresión desde centenares de máquinas repartidas por todo el mundo, como ha ocurrido en las Webs de *Yahoo, Amazon, CNN, eBay, Buy, ZDNet*.

Dado el elevado número de sistemas existentes en Internet, la capacidad de "reclutar" recursos es inmensa. Debido a las vulnerabilidades de los sistemas operativos y de las aplicaciones, como los *Buffer- Overflows* y los *Format-Strings (se especifican más adelante en este documento)*, un atacante es capaz de apoderarse de un conjunto de sistemas (de cientos a miles) e instalar en ellos un servicio que acepte órdenes del atacante para ejecutar un DDoS contra una máquina objetivo.

La sofisticación de las herramientas actuales hace que no se requieran conocimientos técnicos avanzados para llevar a cabo este tipo de ataques.

Las Herramientas por si solas se encargan de analizar y vulnerar los sistemas, para copiarse e instalarse automáticamente (en unos segundos). Dicho proceso está compuesto de 4 pasos principales:

1) Fase de escaneo con un conjunto objetivo de sistemas muy elevado, 100.000 o más. Se prueban éstos frente a una vulnerabilidad conocida.
2) Se obtiene acceso a parte de esos sistemas a través de la vulnerabilidad.
3) Se instala la herramienta de DDoS en cada sistema comprometido.

4) Se utilizan estos sistemas para escanear y comprometer nuevos sistemas.

En el modo de operación genérico de las herramientas de DDoS, el intruso se comunica mediante comandos con un elemento denominado *Handler*. Éste se encarga de gestionar el registro, realizado previamente, de un conjunto de agentes, normalmente elevado en número, que son realmente el origen de los paquetes del DDoS. Por tanto, los agentes y el *Handler* conforman una red de ataque, que actúa en el momento en que el *Handler* retransmite a todos y cada uno de los agentes las órdenes invocadas por el intruso remotamente.

Las comunicaciones entre estos elementos se realizaban originalmente por puertos fijos y, a la larga, conocidos, por lo que este modo de funcionamiento podía ser detectado por sistemas *IDS* con facilidad. La difusión en el uso del IRC o chat, ha dado lugar a la utilización de este medio (y sus puertos TCP asociados, del 6660 al 6669) para constituir los canales de control de los elementos de un DDoS.

i) *Trinoo:*

Esta herramienta de DDoS, permite el acceso a través de autenticación basada en claves (mediante *Crypt ()*), y a su vez, permite determinar si un binario concreto de una máquina actúa como maestro o como esclavo. Inicialmente surgió por la explotación de un *buffer-overfow* en los sistemas que actuaban de víctimas. Existe una versión asociada a Windows, llamada *WinTrinoo*.

j) *Direct Broadcast:*

Este tipo de tráfico puede dar lugar a la existencia de redes amplificadoras de tráfico empleadas en ataques de tipo DoS como *Smurf*. Existen otros tipos de paquetes de broadcast que permiten a un atacante extraer información valiosa de la red y su composición. Mediante el uso de paquetes broadcast de máscara de red, un atacante puede obtener los bloques de redes empleados para posteriormente emplear rangos de IPs precisos en sus escaneos. Asimismo, mediante la utilización de Broadcast de tipo *timestamp*, el atacante puede extraer información de identificación de los sistemas existentes.

k) DNS:

El DNS es una fuente de información de red muy valiosa. DIG es una utilidad para la obtención de información del servicio de nombres DNS, permite copiar una base de datos entera de nombres (dominio) desde un servidor DNS, para su posterior análisis. Asimismo sus características avanzadas facilitan extraer toda la información asociada al protocolo DNS, no permitiendo únicamente la realización de peticiones, como *nslookup*.

l) NTP:

El protocolo NTP, Network Time Protocol, permite sincronizar la hora de forma simultánea en todos los equipos de una red. Este protocolo presenta diferentes vulnerabilidades, ya que por ejemplo, los sistemas de alta disponibilidad configurados en cluster se basan en el momento horario de cada uno de sus nodos para gestionar el cluster que ofrece el servicio. En el caso de poder modificar la hora en un nodo, podrían obtenerse resultados inesperados en el

conjunto de ellos, como por ejemplo que se desconfiguraran ciertos nodos, no formando parte del cluster, pudiendo llegar a anularse la alta disponibilidad.

Mediante el comando *ntpdate* se puede modificar la hora de un sistema:

```
# ntpdate –d <<dirección_IP>>
```

Mediante el comando *ntpq* se pueden hacer consultas al servicio NTP de un sistema.

Por ejemplo para ver las asociaciones de un equipo, es decir, de quién obtiene la hora:

```
# ntpq –p <<dirección_IP>>
```

m) Caballos de Troya:

Pese a que esta vulnerabilidad está más asociada a los sistemas y no a la pila de protocolos como tal, es empleada para introducir servicios no deseados en sistemas destino y poder así ejecutar ataques remotos posteriormente o incluso tomar su control por completo.

También conocidos como puertas traseras (*Back Doors*), son fragmentos de programas no autorizados que se introducen en otros para que el programa original ejecute ciertas acciones no deseadas.

En el caso de los Trojanos que afectan a los servicios más directamente, se trata de programas completos, que normalmente se justifican como herramientas de administración remota o RAT (típicamente de Windows) como por ejemplo:

- Back Orifice (http://www.blackhat.com y http://www.cultdeadcow.com/tools/).
- Back Orifice 2000 (http://www.bo2k.com - http://www.bo2k.de).
- NetBus (*http://www.netbus.org*).
- SubSeven (http://www.sub7files.com - http://www.sub-seven.com/).

Asimismo, las herramientas típicas de administración y acceso remoto podrían incluirse en este grupo, ya que facilitan el acceso y el completo control del sistema destino. Entre estas se encuentran *PCAnywhere, VNC (Virtual Network Computing), Windows Terminal Services.*

n) IPSec:

La seguridad del estándar IPSec ha sido analizada en numerosos estudios, poniéndose en entre dicho como característica negativa la complejidad de sus especificaciones y del propio protocolo.
Los dispositivos que “hablan” IPSec pueden ser identificados por tener el puerto 500 escuchando, ya que es el asociado al estándar de intercambio de claves o IKE, Inter Key Exchange Protocol.

o) Finger Bomb:

Es otro tipo de ataque DoS que permite forzar al sistema destino a un consumo elevado de CPU realizando una petición *Finger* recursiva. Para ello se dispone de *scripts* como *kaput* que hacen uso de esta vulnerabilidad.

p) *RPC (Remote Procedure Call):*

Es una tecnología de red creada por Sun *Microsystems*, que permite invocar procedimientos y acciones de forma remota desde otro equipo.
Es posible obtener la lista de servicios activos en un equipo mediante el siguiente comando Unix:

#rpcinfo –p <<dirección_IP>>

g) Relaciones de Confianza entre Sistemas:

Los comandos r-Unix (*rsh, rcp, rlogin*) requieren de relaciones de confianza entre sistemas para accederse entre sí directamente, esquivando los controles de seguridad y autenticación habituales. Esto significa que si se es capaz de vulnerar uno de los sistemas incluidos en el círculo de confianza, se dispondrá de acceso al resto.

Si se desea filtrar del exterior la utilización de estos programas puede hacerse mediante los puertos 512, 513 y 514. Los ficheros implicados en la obtención de permisos son:

/etc/host.equiv, $HOME/.rhosts.allow o /hosts.deny, y .shosts

Por ejemplo, si un atacante es capaz de obtener a través de un exploit uno de estos ficheros, es capaz de ver las puertas de entrada desde las que el acceso está permitido, por lo que su siguiente paso será adquirir el control de alguno de los sistemas contenidos en el fichero. Existen asimismo ataques que se basan en modificar el fichero de confianza, por ejemplo el *.rhost* en */usr/bin*, para poder acceder libremente desde el sistema actual.

r) Buffers- Overflobs:

Los desbordamientos de un buffer, se mencionan, junto a los *Format Strings*, como el último tipo de vulnerabilidad dentro de las asociadas a la capa de aplicación, es ejecutada mediante el envío de paquetes de información desde la red, explotando una debilidad. La primera vulnerabilidad encontrada en Internet de este tipo fue el famoso "*Gusano de Robert Morris, Jr*".

El 2 de noviembre de 1988, éste estudiante generó un exploit que aprovechaba dos vulnerabilidades: la primera asociada al modo de depuración del servicio *sendmail* (que permite el envío de e-mails), y la segunda relativa al servicio *fingerd* (que implementa la identificación mediante peticiones Finger) de los sistemas Unix.

El gusano fue capaz de colapsar por aquel entonces gran parte de los sistemas existentes en Internet, provocando gran conmoción respecto a la seguridad en La Red. Los servidores que proporcionan un servicio TCP/IP u OSI, a través de protocolos de nivel superior, como HTTP, SMTP, FTP, DNS, NNTP, pueden presentar errores de diseño o implementación que dan lugar a vulnerabilidades de seguridad.

Los *S.O* abiertos suelen ser estudiados en mayor profundidad, por lo que las vulnerabilidades existentes son más conocidas, y por tanto, están más controladas por medio de parches correctivos. El mejor ejemplo de un sistema así es Linux. En el caso de S.O propietarios, como por ejemplo la familia Windows, la información al respecto depende del fabricante.

s) Format Strings:

Los ataques de *Format String* se producen al imprimir o copiar a otro buffer un *String*. El programador pretende imprimir su contenido con una sentencia como:

```
printf("%s", str);
```

Pero en su lugar, escribe:

```
printf(str);
```

El resultado funcional es el mismo, pero el resultado técnico es muy diferente, ya que esta sentencia genera un agujero de seguridad en el código que permite controlar su flujo de ejecución. Aunque el programador le indica a la función el *String* a imprimir, ésta lo interpreta como un *String* de formato, es decir, pretende encontrar en su contenido caracteres de formato especiales, como por ejemplo

```
"%d", "%s", "%x".
```

Analizando la función *printf* sobre la que se desarrollará el ataque: aparte de las utilidades propias de la función para imprimir enteros, Strings y delimitar la longitud de los campos a imprimir, ésta permite:

Obtener en cualquier momento el número de caracteres en la salida: al encontrarse un "*%n*", el número de caracteres en la salida antes de encontrar éste campo se almacenará en la dirección pasada en el siguiente argumento:

```
Int valor, x = 100, y = 20;
Printf("%d %n%d", x, &valor, y);
```

El carácter de formato *"%n"* devuelve el número de caracteres que deberían haberse emitido a la salida, y no el número de los que realmente se emitieron. Por ejemplo, al formatear un String en un buffer de tamaño fijo, el String podía ser truncado. A pesar de esto, el valor devuelto por "*%n*" será el desplazamiento si el String no se hubiera truncado:

```
char buf[20];
int valor, x = 0;
sprintf(buf, sizeof buf; "%.100d%n", x, &valor);
printf("Valor: %d", valor);
```

Este ejemplo imprimirá "Valor: 100" y no "Valor: 20".

Por tanto, mediante la manipulación correcta de funciones como *sprintf ()* y *printf ()* se pueden escribir caracteres en la pila, concretamente el número de bytes indicados por "*%n*", en la dirección que se le indique a la función a través del String de formato.

3.2.1.3 ATAQUES A LA CAPA DE TRANSPORTE

Los ataques a la capa de transporte van asociados al funcionamiento de los protocolos TCP y UDP. Escaneo de puertos, inundaciones UDP, DoS por sobrecarga de conexiones, son algunos de los ataques a dicha capa. A continuación se detallan los ataques y vulnerabilidades con más nivel de detalle:

a) Fingerprinting:

Una técnica que permite extraer información de un sistema concreto, es decir; la obtención de su huella identificativa respecto a la pila de protocolos. El objetivo primordial suele ser obtener el sistema operativo que se ejecuta en la maquina destino de la inspección. Esta información junto con la versión del servicio o servidor facilitara la búsqueda de vulnerabilidades asociadas al mismo.

La probabilidad de acierto del sistema operativo remoto en muy elevada, y se basa en la identificación de las características propias de una implementación de la pila frente a otra, ya que la interpretación de los *RFCs* no concuerda siempre. Para poder aplicar esta técnica con precisión es necesario disponer de un puerto abierto (TCP y/o UDP).

b) Escaneo de Puertos – Vulnerabilidades:

Una vez que se dispone de los dispositivos a nivel IP activos en una red (por ejemplo, mediante ICMP), puede aplicarse a cada uno de ellos una técnica, centrada en la posterior búsqueda de vulnerabilidades, basada en una exploración de escaneo de puertos abiertos, tanto UDP como TCP.

El escaneo es la determinación de las características de una red o sistema remotos, con el objetivo de identificar los equipos disponibles y alcanzables desde Internet, así como los servicios que ofrece cada no. Permite saber los sistemas existentes, los servicios ofrecidos por ellos, cómo están organizados los equipos, que sistemas operativos ejecutan, cual es el propósito de cada uno.
De forma general, entre los métodos de escaneo se incluyen técnicas como:

- *Ping sweep*
- *Escaneo de puertos*
- *Firewalking*
- *Trace routing*
- *Identificación de Sistema Operativo*

c) Udp Flood:

El ataque de inundación UDP es una *Denegación de Servicio* (DoS) mediante el *User Datagram Protocol (*UDP). El uso de UDP para ataques de denegación de servicio no es más sencillo que el uso de TCP para el mismo fin.

El ataque de inundación UDP puede ser iniciado por el envío de un gran número de paquetes UDP a puertos aleatorios en un host remoto. Para un gran número de paquetes UDP, los sistemas de las víctimas se verán, obligados a enviar muchos paquetes ICMP. Esto impide que el ICMP sea alcanzable por otros clientes. Además, el atacante puede falsificar la dirección IP de los paquetes UDP, garantizando que los ICMP de retorno no lleguen a su fin.

d) TCP SYN Flood:

Dentro de los ataques DoS, existe uno asociado directamente al protocolo TCP. Consiste en el envío masivo de paquetes de establecimiento de conexión (*SYN*) contra un sistema. La recepción de estas solicitudes provoca que el sistema destino, objetivo del ataque, reserve cierta cantidad de memoria (buffers) para almacenar las estructuras de datos asociadas a cada una de las nuevas conexiones en curso

El protocolo TCP requiere del establecimiento de una conexión, que se realiza en tres pasos. Tras la recepción del paquete SYN, responderá con su paquete SYN-ACK, permaneciendo a la espera del paquete final (ACK) que confirma el establecimiento de la conexión TCP (three-way handshake). La conexión permanece en el estado semiabierto, concretamente SYN_RCVD. El atacante no enviará nunca ese ACK esperado, por lo que la memoria del destino es copada en su totalidad por conexiones falsas, no siendo posible el establecimiento de conexiones de clientes reales, y por tanto anulándose el servicio

e) Connection Flood:

Los servicios TCP orientados a conexión, que son la mayoría (telnet, ftp, http, smtp, nntp) tienen un límite máximo de conexiones simultáneas soportadas; cuando este límite se alcanza, cualquier conexión nueva es rechazada.

De forma similar al Syn Flood, si un atacante es capaz de monopolizar el límite definido con conexiones de su propiedad, que simplemente son establecidas pero por las que no se realiza ninguna comunicación posterior, el sistema no proporcionará servicio.

Al igual que antes, las conexiones expiran progresivamente con el paso del tiempo, pero un ataque constante de apertura de conexiones mantendrá continuamente el límite en su valor máximo. La diferencia está en que en este caso la conexión se ha establecido y por tanto se conoce la identidad del atacante (dirección IP), y a su vez, la capacidad del sistema o sistemas atacante/s debe ser lo suficientemente elevada como para mantener abiertas todas las sesiones que colapsan el servidor atacado.

Existe una variante de estos ataques basada en el uso de un cliente que establezca conexiones contra un sistema, pero que no las finalice de forma correcta, de modo que en el servidor los *sockets* correspondientes a estas comunicaciones seguirán estando activos y consumiendo recursos, concretamente en el estado TCP denominado *TIME_WAIT*.

f) Tribe Flood Network y Tfn2k:

La comunicación entre clientes y servidores se realiza a través de paquetes de ping: ICMP echo Request e ICMP echo Reply, esto posibilita ataques DoS basados en *ICMP Flood*, *SYN Flood*, *UDP Flood*, y *Smurf*, así como obtener una *Shell* de root asociada a un puerto TCP seleccionado.

La comunicación entre clientes y servidores no emplea puertos concretos. Éstos pueden determinarse en el momento de la ejecución o pueden elegirse aleatoriamente en el propio programa, pero consisten en una combinación de los protocolos ICMP, TCP y UDP.

Asimismo añade capacidades de encriptación, eliminando así la detección por los sistemas IDS.

g) Land:

Este ataque permite bloquear un sistema, mediante el envío de un paquete SYN cuya dirección IP fuente y destino es la misma. Existe una variación de este ataque, basada en que los puertos origen y destino también son iguales. Para ello es necesario enviar paquetes IP mediante la técnica de *Spoofing* el cual se ve más adelante en este documento.

Debe tenerse en cuenta que algunos sistemas IDS detectan la primera situación y otros la segunda. Por tanto, podría darse algún caso en el que se establezca una conexión a la propia máquina, se envíe por tanto un paquete:

[127.0.0.1:puerto_cliente ==> 127.0.0.1:puerto_servidor],

Y el sistema IDS lo detecte como un ataque cuando en realidad no lo es. Este ejemplo, aplicable a un gran número de las vulnerabilidades mencionadas, refleja la estrecha línea existente entre un ataque real y una situación convencional, denotando que su detección y automatización no es trivial.

h) Sesión Hijaking:

Considerando la importancia de la información trasmitida a través de las redes de datos, y las medidas de seguridad que deben desarrollarse, esta técnica pretende mostrar la posibilidad de apoderarse de una sesión ya establecida. Este avance podría suponer el obviar todo el proceso de autenticación previo.

El *TCP Hijaking* puede realizarse en entornos de red de difusión, basado en introducir paquetes en medio de una transmisión como si provinieran del dispositivo original (*IP Spoofing*). Este tipo de ataques también se conoce como "*Man in The Middle Attack*", ya que el atacante debe situarse entre el equipo que estableció la conexión original y la víctima.
Para poder tomar el control de una conexión previamente, es necesario obtener la información asociada a cómo transcurre ésta a lo largo del tiempo.

Concretamente en TCP, deben conocerse los números de secuencia actuales, ya sea directamente o a través de los *ISNs* (*Números de Secuencia Iniciales)* y del número de bytes trasmitidos. Una
vez conseguido el control, el objetivo será ejecutar algún comando, típicamente se pretende apoderarse de sesiones de terminal, que permita acceder al sistema remoto de forma directa.

Habitualmente el control de la sesión se realiza empleando técnicas como *Source-Routing*, de forma que los paquetes de vuelta lleguen al atacante y no al destino real. En caso de no disponer de esta facilidad la técnica se conoce como *Blind-Hijacking* y se basa en adivinar o intuir las respuestas de los sistemas que intervienen en la comunicación. Para obtener la información de la conexión existente debe emplearse un *Sniffer*, situándose entre los sistemas que se están comunicando, ataque conocido como "*Man-in-The-Middle Attack*"

i) TCP Initial Sequence Numbers:

El protocolo TCP genera un ISN, o número de secuencia inicial, para poder realizar el control de flujo de la conexión. Este es uno de los ataques más antiguos, data de 1985, y se basa en la utilización de *pseudo-random Numbers*

Generators (PRNGs) para la generación de los ISNs. Si los números de secuencia pueden ser predichos, puede llegar a ser posible el modificar la información de la conexión, apoderándose de ella mediante *Hijaking* o realizar *blind Spoofing* sobre futuras conexiones

La modificación de los datos en la conexión puede realizarse inyectando paquetes válidos, al conocerse el ISN inicial y el número de bytes intercambiado, y por tanto, el número de secuencia actual. Si no se conoce exactamente este valor, pero sí de forma aproximada, puede enviarse también un grupo de paquetes en un rango de secuencia concreto (que vendrá limitado por el tamaño de ventana TCP), con el objetivo de que alguno coincida con el número de secuencia actual.

Se ha encontrado una nueva vulnerabilidad que se presenta cuando se usan incrementos aleatorios, al aumentar constantemente el valor de los ISNs generados. Debido a las implicaciones del teorema del límite central, el sumatorio de una serie de números no proporciona la suficiente varianza en el rango de valores de ISN deseados, por lo que un atacante puede apoderarse de las conexiones. Por tanto, los sistemas basados en la generación de números mediante incrementos aleatorios son vulnerables a ataques estadísticos.

j) Tiny Fragment Attack:

Para comprender este ataque debe considerarse como tiene lugar la fragmentación de paquetes TCP sobre IP. Cuando un paquete IP supera el tamaño máximo de transmisión, MTU, debe dividirse en paquetes menores. El primero de ellos incluirá la cabecera TCP asociada al paquete original, mientras que el resto de fragmentos simplemente contendrán la cabecera IP y los datos, pero no información de la cabecera TCP. A través del campo de *Fragment offset*

de la cabecera IP se determina si existen más fragmentos y la relación entre éstos.

Cuando se gestiona un sistema de filtrado de paquetes, lo habitual es permitir que los fragmentos de un paquete IP pasen el filtro, ya que no se dispone de información TCP para tomar una decisión de filtrado en función, por ejemplo, de los puertos origen y destino.

k) Winnuke:

Este ataque afecta a los sistemas que utilizan el protocolo *NetBIOS*, típicamente en el sistema operativo Windows. Este protocolo emplea los puertos UDP 137, 138 y 139. El envío de un paquete urgente (bit URG=1), conocido como paquete "*Out of Band" (OOB*) da lugar al envío de datagramas UDP a estos puertos, que al intentar ser enviados a las capas superiores, pueden provocar que el sistema destino se "cuelgue" o que disminuya su rendimiento de forma notable

l) Teardrop:

El ataque *Teardrop* se basa en el envío de fragmentos de paquetes en lugar de paquetes completos. Se comprobó que algunas implementaciones de la pila de protocolos no eran capaces de reconstruir paquetes con fragmentos cuyos bytes se superponen. El resultado es de nuevo que el sistema destino puede llegar a bloquearse. Este ataque apareció en Linux inicialmente. Para llevarlo a cabo bastaría con 2 paquetes, A y B, dónde el *offset* del paquete B indica que comienza dentro del paquete A

Existen dos versiones de este ataque:

Teardrop y *teardrop2*. La variación de la segunda respecto a la primera se basa en la inclusión de "*Flag de Urgencias* (URG)" en la cabecera TCP de los fragmentos. Por ejemplo, Windows NT 4 SP3 se parcheó frente a la primera versión, pero era vulnerable a la segunda.

3.2.1.5 ATAQUES A LA CAPA DE RED

La capa de red no está exenta de los ataques que usuarios o hackers efectúan contra las vulnerabilidades del modelo OSI. A continuación se presentan los principales ataques o vulnerabilidades.

a) Footprinting:

Para lograr hacer un ataque o un acceso indebido a algún sistema conectado por medio de redes, lo primero que se debe hacer es tener algunos datos relevantes con el fin de saber cuál es el camino que se debe seguir, por lo general este ataque es el primero que prueban los hacker para recopilar información sobre la red como: el Rango de la Red y Sub Red, los puertos abiertos y las aplicaciones que los utilizan. También saber el o los sistemas operativos que corren en los equipos, direcciones IP específicas entre otras.

Pero no todo es malo, por ejemplo un administrador de red también puede apoyarse en este para saber qué información maneja su red y estar atento a las posibles amenazas a las que está expuesta su información.
Para la adquisición de la información necesaria es tan sencillo como utilizar comandos clásicos para obtenerla como: *ping nslookup*, *Traceroute*, *whois*, *Finger, rusers*, *rcpinfo*, *telnet*, *dig*, *nmap*, etc.

b) Escaneo Basado en el Protocolo ICMP

En todo sistema es necesario analizar los usos indebidos que se le pueden dar al escaneo de un sistema remoto, utilizando técnicas basadas en protocolos ICMP como:

c) ICMP Echo:

Esta técnica es usada para identificar todos los equipos existentes en una red, generalmente se acceden a estos datos desde Internet.

Mediante paquetes ICMP como *Echo (8)* y Echo *Reply (0),* se sabrá si existe actividad de alguna dirección IP o no.

Para llevar a cabo esta técnica se utilizan variedad de herramientas como:

- *Fping*
- *Gping*
- *Nmap*
- *Pinger de Rhino9*

d) ICMP Broadcast:

Esta técnica es usada en las variantes de UNIX, los sistemas operativos de Microsoft no responden a este tipo de paquetes

Existen otro tipo de técnicas más avanzadas utilizando protocolos ICMP pero sin utilizar echo, tales como:

e) ICMP Timestamp:

Con protocolos ICMP de tipo *Timestamp*, se podrá conocer la referencia de tiempo en el sistema de destino, pero no todos los sistemas Windows responden a este tipo de paquetes, a diferencia con sistemas basados en UNIX donde si son implementados.

f) ICMP Information:

Su función es permitir que ciertos equipos, que no poseían disco del que extraer su propia configuración, pudieran auto configurarse en el momento de su arranque, principalmente para obtener su dirección IP.

g) ICMP Address Mask:

Aquí los equipos o estaciones de trabajo sin disco, podrían obtener la máscara de red asociada a la subred en la que estaban conectados en el momento de arrancar, se supone que un sistema no debería responder, con un paquete de este tipo, salvo que fuera un agente autorizado para notificar la máscara, típicamente el Router de la subred.

Mediante esta información un atacante puede conocer la estructura interna de la red y el esquema de enrutamiento empleado.

También es posible encontrar un equipo en una red mediante herramientas más avanzadas, que permiten observar el comportamiento de las implementaciones del protocolo ICMP, en otras palabras analizando los mensajes de error de ICMP.

De manera general los métodos a emplear incluyen:

- Modificación maliciosa de la cabecera IP de un paquete, por ejemplo cambiando el campo de la longitud de la cabecera, o los campos de opciones del protocolo IP.
- Uso de valores inválidos en los campos de la cabecera IP.
- Posibilidad de Abusar de la *Fragmentación*.
- Emplear el método de escaneo basado en el protocolo UDP: Es el protocolo ICMP el que se encarga de notificar las anomalías de este.

h) IP Bad Headers Fields:

Este genera un error *ICMP Parameter Problem,* este mensaje se obtiene cuando un Router o sistema procesa un paquete y encuentra un problema con los parámetros de la cabecera IP que no está contemplado en ninguno otro mensaje de error ICMP.

Los Routers deberían detectar este error pero no todos ellos comprueban que ciertos campos de la cabecera IP son correctos, pero es posible de acuerdo a su comportamiento identificar el fabricante del mismo.

i) IP Non-valid Field Values:

Un paquete IP se puede modificar con el fin de que contenga valores no validos en alguno de sus campos, en este caso se genera un error *ICMP Destination Ureachable* cuando se recibe un paquete modificado.

j) IP Fragmentation:

Se genera un mensaje de error *ICMP Fragment Reassembly Time exceded*, si se recibe el paquete ICMP de tiempo excedido al reconstruir los fragmentos, quiere decir que el puerto está disponible y sin filtrar.

k) IP Spoofing:

Se basa en la generación de paquetes IP con una dirección de origen falsa, se puede hacer envío de paquetes con este tipo de direcciones para que desde la misma maquina se disponga de un sistema destino objetivo, porque existe un dispositivo de filtrado que permite el tráfico de paquetes con esta dirección de origen, o porque existe una relación de confianza entre esos dos sistemas.

l) *SMURF:*

Este ataque se aprovecha de las bondades de una dirección *broadcast*, cuando un atacante tiene la opción de enviar un paquete de datos a dicha dirección, puede provocar que todos los sistemas pertenecientes a dicha red respondan simultáneamente.

Pero si se asocia esta técnica con *IP Spoofing*, al enviar un paquete ICMP con la dirección IP de origen de la maquina a atacar y dirección de destino la dirección de *broadcast* de una red con un elevado número de máquinas, todas las repuestas de la red de *broadcast* se dirigirán realmente a la dirección IP del sistema "spoofeado". Este ataque es realmente denominado *SMURF*.

m) *Stacheldraht:*

El alambre de púas, es una herramienta de denegación de servicio, combina características de *Trinoo* y *TFN (Tax File Number)* y añade mecanismos de cifrado en las comunicaciones entre el cliente y el conductor, así como mecanismos de actualización automática de los agentes.

n) *Ping of Death:*

El ping de la muerte, funciona enviando un paquete de ping tan grande que puede ocasionar que el buffer de memoria se desborde, el resultado obtenido puede ser el reinicio de la maquina o el apagado.

Para realizar este ataque es necesario disponer de una herramienta que lo implemente o modificar el límite impuesto en el código fuente del cliente de ping.

o) *Routing Protocols:*

En este ataque se aprovecha las vulnerabilidades de los protocolos de enrutamiento, de tal forma que se introducen paquetes de actualización de rutas, pudiendo así manipular los caminos por donde seguirá el tráfico de acuerdo a las intenciones del atacante.

Uno de los protocolos que se puede adulterar es *RIP* en sus dos versiones, como se trata de un protocolo UDP acepta paquetes de cualquier sistema, sin necesidad de conexión previa.

p) *Source Routing:*

Con esta propiedad de protocolo IP se puede enviar dentro del mismo paquete de datos la información necesaria para su enrutamiento, en materia de seguridad se puede considerar que un ataque es capaz determinar la trayectoria que deben tomar los paquetes, violando las reglas de enrutamiento establecidas en los en los equipos de una red.

q) *ICMP Redirects:*

Existe un tipo de paquete ICMP que es empleado por los dispositivos de enrutamiento, para informar de las alternativas de rutas por las que debe dirigir el tráfico en un sistema ejecutando el protocolo IP.

La vulnerabilidad asociada a esta funcionalidad se basa en generar paquetes de redirección hacia un sistema objetivo, de forma que se oriente su flujo de tráfico hacia sistemas controlados por el mismo atacante.

Realmente si un sistema acepta la recepción de este tipo de paquetes, lo que hace es actualizar su tabla de rutas con una entrada de tipo dinámica, que le indica la nueva ruta a seguir.

r) *Loki:*

Tiene como objetivo la posibilidad de encubrir tráfico en túneles ICMP y UDP, en el caso de que este tráfico este permitido a través de los *Firewalls*, el ataque es posible.

En otras palabras el ataque debe introducir tráfico encubierto generalmente IP, en paquetes ICMP o UDP, que son permitidos. La herramienta consta de un cliente

Loki y un servidor *Lokid* que se encarga de encapsular y des encapsular el tráfico en ambos extremos.

s) *Ataques al Protocolo SNMP:*

El protocolo SNMP, Simple Network Management Protocol, también conocido como “Security Not My Problem”, al menos hasta la versión 3, permite la gestión y administración de dispositivos de red: *RFC 1157* (versión 1) y *RFC 1446* (versión 2). La seguridad de la primera versión se basa en el uso de claves conocidas como *community names*, mientras que la versión 2 gestiona la integridad mediante el uso del algoritmo *MD5*, y permite encriptación, mediante *DES (Data Encryption Standard)*, pero ésta no limita el uso de claves simples.

La versión 3, RFC2570, profundiza más en la seguridad de los dispositivos. A grandes rasgos existen dos tipos de comunidades: *lectura (RO)* y *lectura-escritura (RW)*. Cada clave asociada permite realizar la operación referida, por lo que la clave *RW* permitiría modificar la información del dispositivo de red, mediante el comando *snmpset.*

Los routers suelen disponer de agentes SNMP con grandes cantidades de información acerca de la red debido a su función y situación, por lo que constituirán uno de los objetivos principales de un escaneo SNMP.

Para explotar las vulnerabilidades asociadas a este protocolo, basta con disponer de una utilidad como snmpwalk, disponible para numerosos sistemas Unix, que permite obtener la información almacenada en la *MIB (Management Information Base)* de un sistema conectado a la red de forma remota. En el caso de que las comunidades de lectura y escritura del sistema no se hayan modificado, dispondrá de las establecidas en el estándar, que son respectivamente “public” y “private”.
Podrá obtenerse información de cualquier objeto de la MIB como sigue (en Unix):

```
# snmpwalk <<dirección_IP | nombre_host>> COMUNIDAD [id_objeto]
```

Por ejemplo, para obtener la información de los interfaces de red de un equipo:

```
# snmpwalk host99 public interfaces
```

3.2.1.6 ATAQUES A LA CAPA DE ENLACE DE DATOS

Los ataques a la capa de enlace de datos[22] se centran en el protocolo *ARP (Address Resolution Protocol)*, VLAN y en *STP (Spanning Tree Protocol)*. A continuación se mencionan:

a) Ataques Basados en ARP y CAM:

Puesto que ARP no proporciona seguridad o algún mecanismo para reservar direcciones IP o MAC, se pueden presentar los siguientes ataques:

ARP Spoofing: Es una técnica usada para infiltrarse en una red Ethernet conmutada (basada en *Switch* y no en *Hubs*), que puede permitir al atacante husmear paquetes de datos en la LAN, modificar el tráfico, o incluso detener el tráfico. El atacante envía mensajes ARP falsos o falsificados a la Ethernet, con la finalidad de asociar la dirección MAC del atacante con la dirección IP de otro nodo (nodo atacado), un ejemplo puede ser la puerta de enlace *Gateway.*. Cualquier tráfico dirigido a la dirección IP de dicho nodo será enviada al atacante en vez de al destino original.

Switch Port Stealing (Sniffing): Utilizando ARP Spoofing el atacante consigue que todas las tramas dirigidas hacia otro puerto del switch lleguen al puerto del atacante para luego re-enviarlos hacia su destinatario y de esta manera poder ver el tráfico que viaja desde el remitente hacia el destinatario.

[22] MARRO, Guillermo Mario. Attacks at the Link Layer. California, 2003. p. 12-14

Man in The Middle (Sniffing): Utilizando ARP Spoofing el atacante logra que todas las tramas que intercambian las víctimas pasen primero por su equipo, inclusive en entornos manejados por Switches.

Secuestro (Hijacking): Utilizando ARP Spoofing el atacante puede lograr redirigir el flujo de tramas entre dos dispositivos hacia su equipo. Así puede lograr colocarse en cualquiera de los dos extremos de la comunicación (previa des habilitación del correspondiente dispositivo) y secuestrar la sesión.

Denial of Service (DoS) por ARP Spoofing: Utilizando ARP Spoofing el atacante puede hacer que un equipo crítico de la red tenga una dirección MAC inexistente. Con esto se logra que las tramas dirigidas a la IP de este dispositivo se pierdan.

CAM Table Overflow: Los Switches guardan las asociaciones MAC-Puerto e información de *VLANs* a medida que las "aprenden" en un tabla llamada tabla CAM. La tabla CAM de un switch tiene un tamaño fijo y finito.

Cuando la tabla CAM no tiene espacio para almacenar más asociaciones MAC-Puerto, envía a todos los puertos las tramas que tengan una dirección MAC destino no almacenado en la tabla *CAM.* (Actúa como un *Hub* para cualquier MAC que no haya aprendido).

Existe un ataque teórico desde Mayo de 1999 que se basa en el tamaño limitado de la tabla CAM. Para realizar el ataque sólo hace falta enviar un gran número de tramas con direcciones MAC distintas (usualmente generadas al azar) a cualquier puerto del switch hasta que se llene la tabla CAM y así hacer que envié las tramas por todos los puertos.
Se desarrolló una herramienta para tal fin llamada *Macof* en Mayo de 1999. Actualmente es parte del paquete Dsniff (GNU/Linux).

b) Ataques Basados en VLANs:

Los principales ataques[23] basados en VLANs y DTP son los siguientes:

VLAN Hopping Attack: Un equipo puede hacerse pasar como un switch con 802.1Q/ISL y DTP, o bien se puede emplear un switch. El equipo se vuelve miembro de todas las VLAN. Este ataque requiere que el puerto este configurado con el modo Trunking "automático".

Double Tagged VLAN Hopping Attack: Se envía una trama 802.1Q de la VLAN de la víctima dentro de otra trama 802.1Q de la VLAN local. Los Switches realizan un solo nivel de des encapsulado y solo se permite tráfico en una sola dirección. Este ataque sólo funciona si la VLAN nativa del Trunk es la misma a la que pertenece el atacante y sin importar si puerto del atacante tenga desactivado el Trunking.

c) Ataques Basados en R/STP:

Con la falta de autenticación en los mensajes BPDU en STP y RSTP[24], y el requisito de que todos los Switches tienen que volver a calcular el algoritmo cada vez que se detecte un cambio en la topología, sería factible que un intruso pueda llevar a cabo cualquiera de los siguientes ataques de los recursos de red:

Ataques de Inundaciones:

[23] ARELLANO, Gabriel. Enterprise Security & Risk: Seguridad en Capa 2. p.11,19-23

[24] MARRO, Guillermo Mario. Attacks at the Link Layer. California, 2003. p. 12-14

Estos ataques pueden ser mejor caracterizados como ataques de inundaciones de fuerza bruta. Enviando un diluvio constante de BPDU falsas provocando el cálculo continuo del árbol de expansión, creando así una condición de denegación de la potencia computacional de los switches. Cuanto mayor sea el ancho de banda del ataque, existen más oportunidades de ser exitoso. Hay varias versiones de este ataque que se mencionan a continuación:

- Inundación de la configuración de mensajes BPDU con “bandera TC” encendida. (Inundación de mensajes de configuración de BPDU con bandera TC)

- Inundación por notificación de cambio de BPDUs en la topología. (*TCN por sus siglas en inglés*)

- Inundación de mensajes de configuración BPDU suplantando el puente raíz

Ataques de Compromiso de Topología:

En esta categoría de ataques, una estación que está siendo servida por los Bridges, maliciosamente toma un papel activo en la topología del árbol. Las versiones de este ataque se mencionan a continuación:

Petición del rol de raíz Single-homed: Dentro de unos periodos de tiempo “Hello” cortos, el atacante es capaz de obtener el rol de raíz en un árbol de expansión, independiente de cual sea el switch objetivo de la estructura del árbol. El volcado de captura TCP en los diferentes niveles del árbol no muestra ninguna indicación de anomalías en el protocolo, aparte del hecho de que un switch que previamente no existía, ha obtenido el rol de raíz.

Petición del rol raíz Dual-homed: El atacante se acopla a un host multi-homed (que tiene una aplicación falsa). El anfitrión dice ser la nueva raíz en la topología y sólo se requiere de un mensaje falso por cada periodo de tiempo de saludo. Este ataque es una variación del *Man-in-The-Middle (MITM).*

Entre otras acciones maliciosas, la nueva raíz puede fallar deliberadamente para propagar mensajes de notificación de cambio de topología (tanto para los protocolos *STP y RSTP*).

Petición del rol del Nodo Interno: El atacante sostiene un rol que no necesariamente debe ser el de raíz en el árbol de expansión, en virtud de una parte del estado (aunque corrupto) de la aplicación de los protocolos. Cuanto más se acerca se encuentre el atacante a la raiz, mejores serán sus posibilidades de espiar grandes volúmenes de tráfico. Si el atacante sostiene un papel activo que no sea la raíz del árbol de expansión, la semántica de los protocolos tiene que ser controlada en toda la red con el fin de detectar este tipo de ataque.

Segmentación de Árbol: Los estándares asumen que todos los ID de puente son distintos. Si dos o más puentes cómplices reivindican al mismo tiempo el papel de raíz (mediante el suministro de su propia ID de puente menor que la ID del raíz actual), algunos puentes se confundirán sobre la dirección de los puentes raíz y los segmentos de la topología de red.

3.2.1.7 ATAQUES A LA CAPA FÍSICA

Los ataques a la capa física van enfocados a daños provocados en los dispositivos que pertenecen a la red. Desde una simple desconexión de cable UTP hasta un incendio provocado se puede considerar un ataque a dicha capa.
Un ataque a los sistemas físicos de una red de comunicaciones puede ocasionar una sucesión de problemas que pueden incluso causar mayor impacto que los ocasionados en la parte lógica de la misma. Por ejemplo los ataques físicos a una granja de servidores pueden desestabilizar completamente a todo un sistema de información, más aun cuando no se tiene algún tipo de respaldo a los datos y una medida alternativa de ofrecer los servicios.

Como no es el objetivo de este documento hablar de los tipos de ataques físicos a los elementos electrónicos de una organización, no se tocará a fondo dichos ataques, sin embargo es importante tenerlos en cuenta y no olvidar su importancia dentro del correcto funcionamiento de la organización.

NOTA: Los ataques de la Capa de Aplicación, Enlace Transporte y de Red fueron extraídas al pié de la letra de **[20].**

ANALISIS DE IMPACTO Y FORMAS DE PREVENCIÓN

4.1 IMPACTO DE LOS DIFERENTES ATAQUES A UNA RED DE COMUNICACIONES DE UNA ORGANIZACIÓN

No son solo datos!, a diferencia de elementos físicos como muebles y enseres, o equipos computacionales, la información es caracterizada por ser uno de los activos más importantes con los que una compañía puede contar y enfocar su funcionamiento a la consecución de los objetivos institucionales.

Pero el manejo de la información no es algo fácil, habitualmente nunca se está exento de percances que atenten contra ella. Tanto para la información en medio físico como en medio digital siempre existirá el riesgo inminente de que se pueda perder, riesgo que no se puede correr ya que se atentaría también contra la integridad de las organizaciones o empresas.

Cuando se habla de medio físico, lo que se quiere expresar es toda esa información plasmada en los papeles, el cual en la actualidad se sigue manejando, por una cierta confiabilidad y soporte que brinda. Aunque tiene sus beneficios y sus riesgos la era tecnológica ha cambiado la forma de tratar la información.

Lo que antes era exasperante para los usuarios en el manejo de información, es decir llevar una contabilidad en un libro, realizar una factura manual o simplemente el presentar informes con la posibilidad de contener errores por caracteres mal escritos, ahora es un trabajo que los avances tecnológicos han logrado minimizar en una gran proporción.

Ese tipo de acciones que antes se hacía por medio de “papel y lápiz” ahora es un trabajo que se torna mucho más sencillo y confiable, donde los *SI (sistemas de información)* tienen el papel protagónico.

Para las Organizaciones el arribo de las nuevas tecnologías actuó como impulsor sobre el alto grado de competitividad en el mercado.

Pero no todo es color de rosa, la era digital también trajo consigo su espina, el aumento de acceso a las computadoras y medios de red por parte de usuarios, permitió que mentes pérfidas desearan de forma ilícita el acceso a la información. Además las redes e internet se volvieron el canal de comunicación entre empresas y usuarios, hoy en día es el medio número uno por donde miles de personas en todo el mundo realizan sus transacciones y los hackers sus fechorías.

Las más afectadas son las organizaciones. No importa si es grande mediana o pequeña, si ésta posee un sistema de comunicación interno por la cual circula su información, eso es lo realmente relevante para los intrusos o usuarios que pretendan aprovecharse de todas las factibles debilidades que posee un sistema de red.

Los fines!, obtener información, o hacer daño a empresas que se encuentran en su punto de mira, los motivos!, pueden ser muchos, pero el medio (la redes), el caso de estudio de este documento, es un tema trascendental para minimizar las vulnerabilidades tecnológicas que una empresa pueda tener. No solo los antivirus o firewalls deberían considerarse como escudos en defensa contra los ataques.
Los administradores de los sistemas de información son los encargados de velar por la buena circulación de la información y el buen funcionamiento de los medios (redes de datos), con el objetivo de mantener las organizaciones lejos del alcance de los atacantes.

En otras palabras, es no afectar el bolsillo de las Empresas, ya que es esto lo que realmente se toca, si en algún momento se presentase algún caso de intrusión por parte de piratas informáticos. Muchas empresas a diario facturan millones de pesos, surge entonces un interrogante dentro de muchos otros, ¿es mucho el

dinero que se pierde en un día si se deja de facturar? La respuesta es afirmativa, si un ataque informático independiente de cual sea evita que se desarrollen las labores normales de una compañía seguramente puede estar tocando las ganancias de esta.

4.1.1 IMPACTO DE ACUERDO AL TIPO DE ACTIVIDAD DE UNA ORGANIZACIÓN

Partiendo de la base de que las empresas industriales son las encargadas de la extracción y transformación de la materia prima, las comerciales de compra y venta de productos, y las de servicios se encargan de vender productos intangibles, se pretende asociar los diferentes ataques informáticos a las actividades económicas mencionadas con el fin de construir un panorama amplio del impacto operacional que afecta la economía de las organizaciones.

4.1.1.1 IMPACTO EN LOS PROCESOS INDUSTRIALES

Dentro de los ambientes empresariales la tecnología ha tenido gran acogida, sobre todo en aquellas áreas donde la intervención del ser humano puede ser sustituida por los comandos que da un ordenador (pc) a muchas herramientas que aportan a la producción de algún bien, esto con el fin de disminuir costos. Sin embargo donde existe la intervención de sistemas computacionales también cabe la posibilidad de que sean vulnerados. En otras palabras, que personas maliciosas intenten acceder a los equipos en busca de cometer algún acto delictivo que perjudique la organización.

Para este caso, Imagine una empresa donde sus áreas automatizadas son parte esencial de una línea de producción, súmele, que sus máquinas son en su totalidad autónomas solo necesitan una estación de trabajo programada y las maquinas harán un proceso sin intervención humana. Ahora bien, esta máquina

también consta de una conexión a una red de datos, para poder ser programada remotamente o seguramente algún mantenimiento. Esta conexión se podría clasificar como “la conexión de la muerte” ya que se expone la maquina a las amenazas de las redes, pero no se puede hacer nada para evitarlo, la conexión es indispensable, lo que si es factible de hacer, es prevenir esas amenazas a los posibles ataques.

Dependiendo de la máquina y el software que posea, los ataques pueden variar entre la capa física y la capa de enlace de datos.

No yendo muy lejos, de acuerdo con el artículo de la revista *Technology review.es,* del 26 de octubre del 2011, donde se hace mención de un virus tipo gusano llamado *Stuxnet*[25] el cual realizó daños a maquinas industriales (centrifugadoras de uranio), el virus dentro de su alcance tiene la facultad de reprogramar hasta los PLC (Programming Logical Controller, o Controladores Lógicos Programables), temas como este tienden a ser muy delicados aún más si se trata de ataques contra sistemas gubernamentales trayendo como resultado una posible ciberguerra.

4.1.1.2 IMPACTO EN PROCESOS COMERCIALES

El comercio es un sector muy importante que con el pasar de los años se ha convertido en un negocio muy rentable, por ello las empresas han optado por sofisticar cada día los procesos que deben realizar.
Teniendo en cuenta la importancia de cada proceso, se debe reconocer que un ataque podría ser perjudicial, por esta razón las organizaciones deben anticiparse

[25] TALBOT, David, INFORMÁTICA: Un nuevo software malicioso nos acerca un paso más a la cirberguerra. [en línea]. <http://www.technologyreview.es/read_article.aspx?id=38970 >. [Citado el 8 de Marzo de 2011].

al impacto que puede provocar dichas intrusiones. Por ejemplo la pérdida de información de clientes, o datos que sean relevantes para la empresa. Las cuales podrían llegar a ser muy beneficiosas para otra compañía de la competencia o simplemente por ociosidad, o deseo de cambiarlos.

Esta clase de consecuencias se deben a que no se toman las medidas necesarias de seguridad, por lo que vuelve al sistema vulnerable.

Un claro ejemplo de esto es el fin con que el grupo *Anonymous* hace sus ataques a los sitios web, es decir, la intención de ellos es bloquear durante un tiempo determinado una página que consideren afecta sus intereses.

En cuanto al código malicioso, es un ataque al cual se está expuesto en todo momento, este se presenta de una manera silenciosa que consiste en activar un *playload* que contiene instrucciones dañinas, ocasionando daños graves en los dispositivos del sistema, eso contando con que hay posibilidad de seguir incurriendo en el ataque, causando retrasos y demás inconvenientes para un sistema que se esté utilizando.

Así como los ataques anteriormente mencionados, existe una cantidad de ellos que pueden afectar el funcionamiento de procesos comerciales y con versiones mejoradas de ellos, esta es la razón por la que el documento se vuelve útil a la hora de investigar a que está expuesta una red de una organización, donde lo que más importa es la confidencialidad de los datos.

Muchas empresas en la actualidad han optado por las ventas a través de internet, ofreciendo una gama amplia de artículos mostrados en los catálogos web, posibilitando las compras y las ventas online.

Para realizar este tipo de procesos comerciales, se han implementado una serie de servicios en los portales web, de tal forma que los usuarios puedan realizar sus transacciones de esta forma, sin necesidad de algún tipo de contacto físico entre sí. Dichos procesos hacen alusión al denominado "*E-Tailing".*

El E-Tailing, entonces, requiere que los usuarios estén registrados y que hayan medios de pago online utilizando tarjetas de crédito. De esta forma se generan una gran cantidad de vulnerabilidades asociadas a este tipo de negocio, pues las transacciones electrónicas que allí se generan, requieren de una completa seguridad en la verificación y autenticación de los datos personales de los usuarios.

En dichos procesos electrónicos se podrían generar varios ataques informáticos asociados al robo de información, ataques tales como DNS Spoofing o suplantación de identidad por nombre de domino, en donde el atacante puede tener un dominio falso (empresa de ventas online), el cual tenga las características de una empresa legalmente establecida con todos los servicios que esto conlleva. De esta forma el usuario víctima accede a dicha página y deja sus datos personales, entre los cuales se encuentra el número de la tarjeta de crédito, contraseñas, nombres, cédulas, etc.

Otro tipo de ataque que puede afectar los procesos comerciales de E-Market, es el de SMTP Spoofing y Spamming, pues un atacante puede tener un negocio que requiera de publicidad en la web y se dedique a generar spam pero cambiando su dirección IP de origen, imposibilitando así su detección por el servidor de correos. De esta manera riega la publicidad por toda la red sin ningún tipo de control. Además si esto lo combina con el DNS Spoofing, colocando en dicha publicidad enlaces a páginas falsas, ocasionaría un daño aún mayor.

Es importante entonces resaltar que los procesos comerciales también están sujetos a muchos ataques informáticos, y como se mostró se pueden combinar creando mayor impacto. El impacto de los ataques informativos a los procesos comerciales de una organización se puede resumir en los siguientes ítems.

- Robo de información Financiera de los Clientes
- Infiltración en procesos de ventas e inventarios de la organización
- Suplantaciones de identidad
- Spaming descontrolado.
- Robo de Información Personal de los Clientes

4.1.1.3 IMPACTO EN PROCESOS DE PRESTACIÓN DE SERVICIOS

La prestación de servicios es una modalidad de negocio en el cual se paga por una especie de alquiler de un objeto intangible, que ofrece un beneficio continuo al comprador. Los servicios más comunes son los de agua, energía eléctrica, alcantarillado, televisión y telefonía entre otros.

En la actualidad con el auge de las telecomunicaciones, los servicios se diversificaron en gran medida, apareciendo nuevas modalidades de estos, entre los cuales se encuentran el Internet, La Telefonía Móvil, Los Viajes con GPS, Televisión y Telefonía Digital, entre otros, mejorando notablemente la calidad de la vida de las personas que los consumen.

Sin embargo dichos servicios no se prestan solos, existen como en todo negocio, una cantidad de empresas y organizaciones que se encargan de hacerlo, utilizando para ello un moderno sistema de información que en gran medida está sumergido en una sólida red de datos.

Así como en las organizaciones industriales y comerciales, los sistemas de comunicación de las organizaciones prestadoras de servicios, también están sujetas a vulnerabilidades y ataques que pueden ocasionar serios daños y la anulación o interrupción indefinida de los servicios prestados.

Una vulnerabilidad que se puede asociar a la anulación de servicios es la de Escaneo de Puertos, pues al conocer los puertos TCP y UDP que se están utilizando se puede determinar qué tipo de servicio se está ofreciendo. De esta forma el atacante puede utilizar alguna herramienta de ataque que impida que el servicio se siga ejecutando por el puerto escaneado. Un ejemplo del lado cliente sería que el host del usuario esté recibiendo un servicio vía HTTP utilizando el puerto 80, y el atacante por medio del escaneo de puertos detecte dicho servicio y proceda a utilizar alguna herramienta de ataque que imposibilite la ejecución del servicio.

Para el lado del servidor sería tan "sencillo" como hacer una "*UDP/TCP Flood*" o inundación de puertos TCP o UDP, explicado con anterioridad, en donde es tanta la cantidad de paquetes UDP o TCP que el atacante envía, que el sistema de la empresa envía muchas respuestas ICMP, denegando las respuestas ICMP verdaderas que le tendría que enviar a un cliente, denegando así su servicio.

Así mismo, se pueden realizar más tipos de ataques en la capa de transporte, afectando las sesiones TCP, enviando paquetes incompletos o modificados, desestabilizando la sincronía del TCP, entre otros. De acuerdo a esto se puede anotar que el impacto a la afección en la capa de transporte en la red de una organización prestadora de servicios, va enfocado mayoritariamente a los siguientes aspectos:

- Reducción del tiempo en una sesión de servicio.

- Interrupción del servicio temporalmente
- Reducción de la calidad del servicio
- Intrusión en el servidor identificando datos técnicos del mismo.
- Intrusión en el tipo de servicio identificando datos críticos del mismo

De igual forma como en la capa de transporte, en la capa de red también se presentan vulnerabilidades y ataques que afectan de manera directa la prestación de servicios, por ejemplo utilizando el escaneo de red basado en ICMP, es posible identificar el tipo y versión del sistema operativo, tipo y fabricante del Router, entre otros, de tal forma que les permita a los atacantes tener una base de conocimiento para realizar un ataque de sabotaje, que conlleve a la anulación del servicio prestado.

Otro tipo de ataque que aqueja a la capa de red en cuanto al tema en cuestión es el IP Spoofing, puesto que muchas empresas dentro de su gama de servicios ofrecidos, asignan un rango de direcciones IP autorizadas a recibir algún tipo de servicio. Por medio del IP Spoofing, el atacante puede hacerse pasar por una dirección IP válida dentro de la red y usurpar el servicio de manera gratuita sin generar ninguna sospecha. De esta manera estaría estafando a la empresa y al usuario a quien le correspondería realmente el servicio.

Se puede entonces definir el impacto de los ataques en la capa red de una red de una organización prestadora de servicios al tener en cuenta los siguientes aspectos:

- Perdida de información y suplantación de identidad
- Prestación de servicios a usuarios falsos y denegación a verdaderos
- QoS (Calidad del Servicio) reducida en gran medida.

4.2 FORMAS DE PREVENCION, DETECCION Y MITIGACIÓN DE LOS ATAQUES EN LAS TOPOLOGÍAS DE RED

4.2.1 PREVENCIÓN: IMPLEMENTADA POR DISPOSITIVOS COMO LOS FIREWALLS

Uno de los mejores métodos para hacerle frente a los ataques informáticos es anticipar su presencia, generalmente los administradores de red se soportan en Antivirus, Antimalware, Antispyware y Firewall, y parches de actualización de los sistemas operativos, aun así la solución no se torna suficiente. El desconocimiento sobre los fundamentos de las redes, más explícitamente el desconocimiento del proceso por el cual los datos tienen que pasar para llegar a su destino, contribuye a dejar muchas vulnerabilidades abiertas.

4.2.1.1 PLANTEAMIENTO DE SOLUCIONES

Lo primero que se debe atacar dentro de los entornos informáticos es la ignorancia, mejor dicho, todo usuario es una probable vulnerabilidad en un sistema de información, más aun cuando este no entiende del tema. El nombre más acertado para este tipo de vulnerabilidad es la ingeniería social, donde la ingenuidad es la principal debilidad.

Como método de prevención para este tipo de ataque, lo más recomendable, es tener como punto importante dentro de las políticas de seguridad de una organización, el conocimiento sobre el valor de la información y como se debe proteger para no tener inconvenientes en un futuro.

Una segunda medida, los antivirus dentro de todos los equipos de una organización son una excelente opción. El pecado se comete, cuando estos solo se instalan y ya, cuando este no se configura con estrictas medidas para que realmente haga su trabajo.

Existen programas como antimalware, o antispyware, para complementar la protección. Pero primero entiéndase la diferencia entre estos dos tipos de protección:

Los malware son software malicioso cuyo objetivo es hacer daños a los archivos de un equipo, o al equipo mismo, dentro de este tipo de ataques se encuentran los gusanos y los troyanos, que dentro del modelo OSI pueden afectar a cualquier capa.

Los spyware son software que se introducen dentro de una maquina con el fin de sacar información sin conocimiento y si consentimiento del usuario.
Ya conociendo esta diferencia se puede concluir que:

Los antivirus por muy buenos que sean, no siempre atrapan o detectan todos los virus, que en la actualidad la lista es demasiado larga, por otro lado algunos antivirus no tienen la habilidad de detectar spyware.

Los antimalware se especializan usualmente en la detección de software malicioso, y puede ser un soporte para los antivirus y viceversa.

Los antispyware se concentran en detectar el software espía, que se aloja o intenta alojarse dentro de algún ordenador, vigilando ese lado para el que algunos antivirus no han sido diseñados.

Todo lo anterior se puede decir que son protecciones que van a nivel de cualquier persona que haga de un equipo computacional una herramienta de trabajo.

Expresado en otras palabras, dentro de las políticas de seguridad de los sistemas de información en una organización, todo usuario debería tener la capacidad de inspeccionar cualquier medio de almacenamiento de información (Discos Duros, Memorias USB, CD´s… etc), o información traída atreves de la red. Si este conocimiento no se tiene se debería capacitar el usuario con el fin de que contribuya a la protección del sistema de información.

Administrativamente, para los encargados de la red, el proceso de prevenir algún ataque va más profundo, desde el conocimiento de los modelos de transmisión de datos (TCP/IP y OSI) hasta las herramientas para poder anticiparse a cualquier tipo de ataque.

Comenzando por la configuración de los equipos como Routers, Switches, Servidores proxy, Firewalls y Wrappers, donde los enrutadores se pueden convertir en la primera línea de defesan contra los ataques informáticos, puesto que están expuestos al tráfico de red externo de forma más directa.

Conociendo la configuración de la red y los protocolos se puede lograr, mediante el uso de reglas ACL (Access Control List) o listas de control de acceso, un control al flujo de datos que pasa por el enrutador de tal forma que el flujo proveniente de una determinada interfaz, pueda ser restringido, mejorando la seguridad de la red.

Existen dos tipos de Switches, los gestionados y los no gestionados, los no gestionados son solo dispositivos brutos que permiten la interconexión de equipos en una red, lo más recomendable dentro de una organización es la adquisición de equipos gestionados, los cuales abren un poco más la visión y el control a los administradores de la red permitiéndoles visualizar el tráfico y los accesos no deseados a esta.

Otra forma de prevenir algún ataque asociado a estos equipos, es la segmentación de la red en subredes de acuerdo a las áreas de las organizaciones, esto con el fin de que si algún área de la organización es atacada, el ataque no se propague de forma fácil a las otras áreas.

Los servidores proxy también pueden actuar como medios de prevención de ataques informáticos que arremeten desde las redes externas. Una buena configuración de los servicios que este opera es mediante reglas ACL, que pueden hacer la diferencia entre dejar o no que un ataque entre en el sistema, con estas reglas también se puede controlar la forma como los usuarios hacen uso de los servicios de internet, generalmente los proxy como firewall extienden su protección hasta la capa de aplicación (capa 7) del modelo OSI.

Ya sea lógico o físico los firewalls también ocupan un lugar muy importante dentro de los métodos de prevención de ataques, restringiendo de forma eficiente esos paquetes que viajan a través de la red y que son de carácter dudoso o malicioso. Dentro de las organizaciones este es un medio de defensa sobre sus activos y su prevención se sostiene entre la capa de red y la capa de transporte.

Como los firewalls, los *TCP wrappers* también suministran control de acceso a una variedad de servicios, tales como SSH, TELNET. Básicamente lo que hace es cubrir la identidad de un segundo programa, llaman al programa protegido mediante llamadas estándar al sistema, se puede usar un solo Wrapper para controlar el acceso a diversos programas que se necesiten proteger.

4.2.2 DETECCIÓN: A TRAVÉS DE HERRAMIENTAS DE DETECCION

A través del tiempo los sistemas se han transformado en las herramientas más utilizadas, incluso hasta el negocio más pequeño cuenta con un sistema de red, que le permita tener un mejor manejo de su información. Pero así como la

tecnología y muchas empresas se han propuesto la tarea de sistematizar todo y evolucionar de una manera muy rápida, también existen otros individuos que han utilizado su inteligencia para atacar las vulnerabilidades que estas herramientas presentan.

El avance tecnológico en las redes es algo que también trae sus desventajas, pues en ellas se encuentra cantidad de información que revela cómo hacer un ataque, y al estar ésta información al alcance de cualquier persona obliga a que aumente el porcentaje de posibles atacantes.

La detección se convierte entonces en un factor muy importante, ya que desde allí se comienza a disminuir todas las molestias que implica un ataque. En un constante monitoreo se puede evidenciar cualquier infiltración a la seguridad y así eludirlo.

La auditoría se ha convertido en un mecanismo de detección muy importante, en ella se descubren las falencias que está teniendo una organización, partiendo de la investigación de los empleados en cuanto a cómo han procedido, tanto interna como externamente, teniendo en cuenta que las estadísticas indican que los ataques parten de errores humanos en su gran mayoría.

Esto se menciona porque hay que tener en cuenta que información tiene cada empleado y si es necesario, hacerlo firmar un documento de confidencialidad que lo comprometa a conservar la información bajo secreto. Es posible que al terminar el contrato un empleado utilice la información en contra de la compañía.

Ahora bien, después de los usuarios vienen los ataques informáticos que ingresan al sistema y se encargan de hacer sus debidos daños, para esto ya existen herramientas conocidas, que por medio de probabilidades, frecuencia y tiempo detectan los ataques que están en el medio, como: *Haystack*, IDES/NIDES,

ADAM, PHAD, ALAD, LERAD, NETAD, los cuales tienen como ventaja que pueden detectar nuevas intrusiones, también existen detectores por medio de reglas como: *Wisdom and Sense* y *Time Based Inductive Machine*. Existen también herramientas por medio de redes neuronales, algoritmos genéticos, minería de datos, Agentes, lógica difusa, entre otros. Lo ideal es que la detección se haga en tiempo real para que las anomalías sean corregidas de inmediato.

Una gran ventaja que tienen los antivirus es que van almacenando en su base de datos un historial de ataques, lo cual permite obtener información sobre los virus para así poder mejorar y corregir problemas anticipándose a ellos, además mejorando la eficacia y eficiencia en cuanto a la seguridad.
También hay que mencionar que estas personas que pretender atacar un sistema están incurriendo en un violación, que en manos de las autoridades deben pagar una condena, así que no solo es detectar el problema, sino seguirlo de tal forma que proporcione información acerca de los delincuentes, para que sean judicializados por su delito.

4.2.3 RESPUESTA: TECNICAS Y HERRAMIENTAS DE MITIGACIÓN

La última etapa del proceso es la respuesta, que consiste en las estrategias de mitigación que se pueden utilizar para hacerle contra parte a los ataques que puedan afectar las topologías de red.

A continuación se presentan algunas estrategias de mitigación[26] a ataques específicos mencionados en el capítulo 3 de este documento:

4.2.3.1 FOOTPRINTING

En este ataque como en muchos otros se deben conocer primero cuales son las debilidades o cual es la información que se está dejando en manos no deseadas. La forma más apropiada es hacer un auto ataque sobre los sistemas que se desean proteger, con la intención de revelar la información que hace vulnerable un sistema.

Para este tipo de acciones se puede usar herramientas como:
Snort: Es un software que permite hacer monitoreo de redes además de funcionar como un IDS (Intrusión Detection System), con el que se puede parametrizar filtros o reglas para *backdoor, DDoS, Finger, FTP, ataques Web, CGI,* Nmap etc.
RotoRouter: Programa diseñado para engañar el Traceroute.

4.2.3.2 FINGERPRINTING:

La mitigación de este tipo de ataque se puede realizar por medio de sistemas IDS (*intrusión Detection Systems*), siempre y cuando la técnica de ataque utilizada opere en modo activo. Si la técnica de ataque opera en modo pasivo los IDS no son suficientes y es necesario utilizar una herramienta llamada *IP Personality.*

El parche de *IP Personality* implementado en Linux (*kernel 2.4*), añade la posibilidad de que la pila de protocolos OSI, disponga de diferentes

[26] PÁEZ , Raúl, Análisis de Seguridad de la Familia de Protocolos TCP/IP y sus Servicios Asociados, 1 ed, 2002. p.23.63-93

personalidades, modificando las características de su tráfico de red según unos parámetros. Para esto debe emplearse cualquier elemento que pueda ser especificado en una regla *NetFilterIPtables:* dirección IP fuente y destino, puerto TCP o UDP, etc.

Con estas herramientas se pueden modificar las siguientes características:

- Valor de los Initial Sequence Numbers (ISN) de TCP
- Tamaño inicial de ventana de TCP
- Opciones TCP: tanto su tipo como su orden en el paquete
- Las respuestas a ciertos paquetes TCP empleados en el fingerprinting
- Las respuestas a ciertos paquetes UDP

4.2.3.3 ESCANEO DE PUERTOS:

Para contrarrestar el escaneo de puertos, existe una herramienta llamada *SNORT* que le hace competencia a la herramienta de escaneo *NMAP.* Si el sistema atacado es Unix, existen utilidades como *scanlogd* que permiten la detección de los escáneres de puertos.

Los *firewalls* suelen incluir un módulo de detección de ataques, aunque no todos tienen la misma prioridad o validez. Por ejemplo, el escaneo basado en SYN puede ser detectado, pero no así el basado en paquetes de FIN. Para poder detectar estos ataques es necesario revisar el resultado de los *logs* de los firewalls, cuyo tamaño suele ser elevado, por lo que existen herramientas que facilitan estas tareas.

4.2.3.4 SCANEO BASADO EN EL PROTOCOLO ICMP

Para mitigar los diferentes ataques que se derivan del protocolo ICMP solo es cuestión de definir y parametrizar los filtros que impiden que los datos que no son necesarios para la funcionalidad de los servicios existentes pasen.

4.2.3.5 SNIFFING, EAVESDROPPING y SNOOPING

La mejor acción para mitigar los ataques de tipo *Sniffing (olfateo de información),* es por medio de la encriptación de la información. Para ello existen herramientas como *Tripwire*, que genera una huella mediante *MD5* de los sistemas de ficheros de un host, y permite detectar cualquier modificación realizada sobre los ficheros o directorios.

Existe otra herramienta denominada *CMP*, que permite detectar interfaces en modo promiscuo (capturando todo el tráfico), puesto que en este modo es en donde los *Sniffers* son más efectivos.

Otra protección contra los *Sniffers* es la de utilizar redes conmutadas en vez de compartidas, donde los Switches segmentan la red para cada uno de los puertos, es decir que si se dispone de un equipo por puerto, un *Sniffers* es capaz solo de visualizar el tráfico destinado al sistema en el que está ubicado.

4.2.3.5 “IDS (INTRUSION DETECTION SYSTEMS*)*

Además de los mencionados parches, una de las herramientas existentes hoy en día que proporciona un mayor control sobre la seguridad son los sistemas de detección de intrusos (IDS, Intrusion Detection System), también conocidos como

NIDS, Network IDS, ya que pretenden contemplar dentro de sus comprobaciones todas y cada una de las vulnerabilidades que se van descubriendo a nivel de TCP/IP y OSI de los servicios de red.

Ciertos IDS permiten la introducción de nuevos patrones (signatures), de forma que es posible ampliar la base de datos de vulnerabilidades en el momento en que aparecen, y no tener que esperar a que el fabricante distribuya una actualización. Por ejemplo, los patrones pueden contemplar situaciones como *source-routing*, la obtención del fichero de *passwords* en el contenido de una operación get de FTP, fragmentación de paquetes ICMP de gran tamaño, entre otros.

La alternativa existente previamente a los sistemas IDS pasaba por realizar análisis exhaustivos de los *logs* del *firewall* o grupo de *firewalls*, tratando de interrelacionar los eventos existentes. El problema de este procedimiento es que en un sistema muy accedido, el tamaño de los *logs* es enorme: cientos de Mbyte. Para asimilar la relación de eventos entre el método tradicional y los IDS, basta decir que un ataque de escaneo de puertos, en el *log* del *firewall* generaría unas 65000 entradas (64K puertos posibles) mientras que en el IDS se reflejará 1 sólo evento: “escaneo de puertos”. Lo mismo ocurriría en el caso de un *SYN Flood*, en el *log* aparecerían, por ejemplo, 10.000 conexiones SYN, mientras que en el IDS se vería 1 sólo evento: “*ataque SYN Flood*”.

Los IDSs suelen conformarse mediante un sistema de gestión centralizado y agentes o monitores remotos que se encargan de analizar el tráfico en los puntos remotos de la red en los que están ubicados. La comunicación entre los agentes y el gestor no se realiza a través del protocolo *SNMP* como ocurre en los entornos de gestión de red, sino que la comunicación se establece de forma más segura,

con métodos de autentificación y codificación. Por ejemplo en el Cisco IDS se realiza a través del protocolo conocido como PO, *Post Office*.

Asimismo, la seguridad de estos sistemas se incrementa al trabajar las interfaces por las que se realiza la monitorización en modo pasivo, es decir, no actúan como destino de ningún tráfico (no disponen de dirección IP), por lo que un atacante no puede detectar su existencia. Los sistemas IDS, como por ejemplo *NFR, Network Flight Recorder, Scanlogd* o *Snort*, disponen de la detección de rastreos basados en ping (*ping sweep*). Asimismo, el control de este tipo de reconocimientos puede llevarse a cabo determinando los tipos de paquetes ICMP permitidos en cada segmento de red: para algunos segmentos será necesario permitir los tipos *ECHO, REPLY, HOST UNREACHABLE y TIME EXCEEDED*, pero no otros.

A su vez, a través del control del tráfico en los routers de los bordes de la red se puede mitigar la obtención de información basada en ICMP, como la franja horaria o la máscara de subred empleada. Los dispositivos Cisco disponen de un sistema IDS simplificado en el S.O. propio o IOS. Éste permite el control de diversas vulnerabilidades, disponiendo de la posibilidad de detectarlas y también de responder a ellas: generando una alarma, descartando el paquete o reseteando la conexión. En el IOS los patrones pueden tratarse con carácter informativo o como ataques. “ [27]

[27] PÁEZ , Raúl, Análisis de Seguridad de la Familia de Protocolos TCP/IP y sus Servicios Asociados, 1 ed, 2002. p.23.63-93

4.2.3.6 IP SPOOFING

Por medio de herramientas como *firewalls* y S*creening Routers* se pueden examinar las IPs que son autorizadas el entorno de red evitando ataques por este método.

Los organismos que realmente pueden evitar el uso de ésta técnica son los propietarios de las redes troncales (Backbones) de comunicación, normalmente *carriers* u operadores de telecomunicaciones (SP, Service Provider), ya que evitan desde su origen que un agresor pueda hacerse pasar por otro usuario. Al actuar de nexo de unión de las diferentes subredes, deben permitir únicamente que el tráfico saliente de cada red al troncal lleve asociada una dirección propia de la red desde la que sale. Así se controla el punto de inicio del IP Spoofing.

En Linux esta vulnerabilidad se pueden tratar con herramientas como *ipchains* o *ACL Access Control List.*

4.2.3.7 SMTP Spamming

Para mitigar este ataque es necesario que los dispositivos de red limiten la cantidad de destinatarios de los correos electrónicos. Algunos servidores de correo como *sendmail* , posee una característica ya definida para evitar este tipo de técnicas.

4.2.3.8 DoS y DDoS

Para mitigar los ataques de denegación de servicios estándar o distribuida, es importante tener en cuenta que dicha mitigación puede ser indiferente del modelo OSI, y puede requerir por lo tanto de un estudio diferente al de este documento. Sin embargo existen herramientas de detección, de intrusos que pueden identificar las huellas dejadas por las herramientas DDoS antes de que puedan terminar satisfactoriamente el ataque.

Se puede lograr una identificación de los atacantes mediante el uso de auditorías y referencias cruzadas de los ficheros *log* y los "*IRCs* de *Hacking"*.

Los ataques DDoS reflejan la necesidad de proteger todos los sistemas de una organización, aunque no contengan información valiosa, ya que pueden ser empleados como fuente de origen para la realización de ataques posteriores.

La defensa más adecuada para este tipo de ataques, consiste en seguir las recomendaciones y prácticas de seguridad: deshabilitar todos los servicios innecesarios, mantener el software actualizado y suscribirse a las lista de correo de seguridad. También es importante no mantener abiertos a todo el internet los servicios de *Proxy,* puesto dichos servicios pueden ser utilizados para generar nuevos ataques o crear una red intermedia para atacar cualquier otro sistema.

Las organizaciones no deben poseer una única puerta de enlace a internet, puesto que será el único punto de acceso en el cual se pueden dañar todos los servicios de un solo golpe.

4.2.3.9 SMURF

Su solución se favorece restringiendo el trafico broadcast que trata de ingresar desde fuera de la red, evitando de esta forma el incremento de tráfico que se genera por este ataque. Para ello se debe bloquear los *Routers* y *Firewalls* de los extremos de la red, pues estos deben ser los encargados de no propagar los *broadcast.*

Las siguientes direcciones Web permiten comprobar si una red es vulnerable a este ataque basado en ICMPs, simplemente introduciendo la dirección de la red a chequear:

http://netscan.org/index.html

http://www.powertech.no/smurf/

En los equipos Cisco, este tipo de ataques puede controlarse mediante una característica denominada "*Unicast RPF".* Esta funcionalidad también elimina otros ataques basados en *IP Spoofing*. Para ello es necesario configurar el siguiente comando de interfaz:

```
(Router-if)# ip verify unicast reverse-path
```

Esta característica comprueba cada paquete que se enruta hacia el enrutador; sí la dirección IP fuente no posee una ruta en la tabla interna *CEF (Cisco Express Forwarding*), que apunte a la misma interfaz por el que llegó el paquete, éste es descartado. Por tanto, es una funcionalidad de entrada que actúa sobre los paquetes recibidos por el Router.

4.2.3.10 TCP Syn Flood

Para el control de este ataque, por ejemplo en los equipos Cisco, se debe tener en cuenta el límite del *ratio* admitido para paquetes SYN. De la siguiente forma se puede configurar dicho parámetro:

```
interface {int}
rate-limit output access-group 153 34000000 100000 100000 conform-action
transmit exceed-action drop
rate-limit output access-group 152 1000000 100000 100000 conform-action
transmit exceed-action drop

access-list 152 permit tcp any host eq www
access-list 153 permit tcp any host eq www established
```

El valor 34000000 representa el valor máximo del ancho de banda del enlace (34 Mbps), y el valor 1000000 se establece con un valor que esté comprendido entre un 50% y un 30% del ratio de *SYN Floods*. Asimismo, deben reemplazarse los "*ratios burst* , normal y "*burst max"* con valores precisos.

Esta parametrización es fundamental para diferenciar situaciones de tráfico habituales de un ataque *SYN Flood* real: sí el ratio de pico se fija a más del 30%, muchos SYN legítimos se descartarán. Para obtener el valor del ratio debe emplearse el comando "*show interface rate-limit*", visualizándose los valores típicos y los excesos de la interface. Por tanto, deben obtenerse los valores habituales en un funcionamiento normal (antes de que ocurra un ataque) y emplear éstos como límite.

4.2.3.11 CONNECTION FLOOD

Para contrarrestar este tipo de ataque, el sistema servidor puede controlar el tiempo que un *socket TCP* puede permanecer en el estado TIME_WAIT, evitando el consumo excesivo de recursos. Para efectuar esto se realiza el siguiente comando:

Linux(2.4): `# echo 512 /proc/sys/net/ipv4/tcp_max_tw_buckets`
Windows NT, 2000, XP:
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters`

4.2.3.12 BASTION HOSTS

La primera regla de oro a la hora de asegurar un sistema host tanto Unix como Windows, es deshabilitar todos los servicios TCP/IP innecesarios. A su vez, son múltiples los controles que pueden llevarse a cabo, tanto desde el punto de vista del sistema como de la red. A continuación se muestran varias configuraciones que pueden ser de gran utilidad para la mitigación de ataques de este tipo:

Para evitar que se responda a peticiones Timestamp

```
TRANSPORT_NAME[5]=ip
NDD_NAME[5]=ip_respond_to_timestamp
NDD_VALUE[5]=0 #
```

Para no enviar mensajes en paquetes de reset de TCP

```
TRANSPORT_NAME[6]=tcp
NDD_NAME[6]=tcp_text_in_resets
```

```
NDD_VALUE[6]=0
```

4.2.3.13 BASTION ROUTERS

Al igual que ocurre con los sistemas, los dispositivos de red deben ser configurados desde un punto de vista restrictivo, de forma que imposibiliten explotar la mayoría de vulnerabilidades comentadas. Para ello se configuran como un *bastion router* .

Las características más importantes a tener en cuenta en cuanto a la seguridad de un *router* son las siguientes:

- Existencia de claves en claro en la configuración.
- Servicios TCP y UDP simples activos: *echo, discard, daytime*.
- Protocolos de Routing sin autenticación y/o encriptación.
- Protocolos AAA sin encriptación.
- Aceptación de paquetes *source routing*.
- Redirecciones IP.
- Proxy ARP.
- CDP, Cisco Discovery Protocol.
- Servidor HTTP activo.

A continuación se mencionan las configuraciones a un router que se pueden realizar de manera genérica para acoger la seguridad de las características antes mencionadas. Para esto es necesario deshabilitar los siguientes servicios:

-Finger:

```
No service finger
```

-Servicios simples: echo,discard,daytime.

```
No service tcp-small-servers
No service udp-small-servers
```

HHTP server:

```
No ip htttp server
```

Proxy ARP: en algunos escenarios, el uso de un proxy ARP puede condicionar a que el tráfico circule por un camino que no es el impuesto por los protocolos de *routing.*

```
No ip proxy-arp
```

4.2.3.14 TRINOO, TRIBLE FLOOD NETWORK, TFN2K, STACHELDRAHT

Mediante la identificación de los puertos empleados por estas herramientas pueden evitarse sus consecuencias y detectarse su existencia. Otras herramientas genéricas de control de DDoS también las detectan, aunque como norma general, el aseguramiento del sistema es la clave. El deshabilitar el tráfico (típicamente ICMP) a través del que se comunican los componentes de la herramienta, también anula su ejecución.

4.2.3.15 STACHELDRAHT

No es fácil darle una solución completa a los ataques de denegación de servicios distribuidos, pero no significa que no se pueda tomar ciertas precauciones para mitigarlos.

Se puede comenzar previniendo el ataque, mediante acciones como:

a) Contar con Servidores Seguros:

La configuración inicial de este dice mucho sobre cuán vulnerable puede ser ante un ataque. De acuerdo a los permisos de instalación, es decir quién y que se puede instalar en un servidor, no cualquier persona debe ser autorizada para hacer debida instalación de programas, o subir o bajar servicios. Por este motivo se debe contar con políticas bien definidas de administración y gestión de contraseñas, contar con un firewall y que sea configurado idóneamente.

b) Filtrado de Paquetes:

Esta acción se puede desarrollar con una apropiada configuración en los enrutadores de una red, descartando el ingreso a la red de paquetes de dudosa procedencia.
Otra método de precaución es teniendo los ojos abiertos ante los posibles ataques, esto se logra poniendo los sistemas a detectar las factibles intrusiones, mediante constante monitoreo a la red, revisión de los archivos de log, análisis periódico de los archivos de configuración entre otros.

4.2.3.16 NAT: NETWORK ADDESS TRANSLATION

La herramienta de traducción de direcciones NAT aporta cierta característica de ocultación "*security through obscurity".* Por medio de esta característica no se permite conocer las direcciones IP reales internas de una red desde el exterior. Esto impide la obtención de información con técnicas como *Footprinting.*

4.2.3.17 PING OF DEATH

La solución generada por los fabricantes de las implementaciones se basa en la generación de modificaciones en la pila de protocolos OSI. En caso de no disponer de un parche asociado al S.O, el ataque puede evitarse filtrando los paquetes ICMP en el *firewall* de entrada, una solución aún más detallada es filtrar únicamente los paquetes ICMP fragmentados, y no todos, ya que otros protocolos o procedimientos pueden emplear paquetes ICMP para otros dispositivos.

4.2.3.18 ROUTING PROTOCOLS

Los protocolos de enrutamiento pueden protegerse garantizando la autenticación del sistema de red que envía la actualización de la tabla de rutas así como encriptado los datos con el objetivo de prevenir la inserción de actualizaciones falsas.

Es conveniente deshabilitar protocolos no seguros como RIP.

4.2.3.19 LAND

Para contrarrestar este ataque se debe inicialmente actualizar la pila de protocolos OSI del S.O con los parches recomendados por el fabricante. Por otra parte es necesario filtrar los paquetes IP *"spoofeados"* de tal forma que queden bloqueados pues no es posible borrarlos.

4.2.3.20 SESSION HIJAKING

Para mitigar este ataque, es útil utilizar las técnicas de encriptación como *IPSec* o *SSH*, las cuales eliminan la posibilidad de obtener información necesaria para reemplazar una sesión con otra.

4.2.3.21 SOURCE ROUTING

Las diferentes implementaciones disponen de mecanismos para deshabilitar ésta característica, de forma que no se acepten paquetes con *Source Routing*.

Para Routers Cisco Mediante el comando "`no ip source-route`" el Router no admitirá paquetes con los datos de ruta implícitos.

En el caso de Windows a través del editor del registro (regedt32.exe) debe localizarse la clave:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
```

Bajo la misma es necesario añadir el valor:

```
Value Name: DisableIPSourceRouting
Data Type: REG_DWORD
Value: 0 , 1 or 2
```

Dónde:

0 - Permite habilitar *source routing*

1 - Deshabilita *source routing* cuando *IP forwarding* está activo

2 - Deshabilita *source routing* completamente (más seguro).

4.2.3.22 ICMP REDIRECTS

Las implementaciones TCP/IP y OSI disponen de mecanismos para controlar y deshabilitar la gestión de este tipo de paquetes, ya que mediante los mismos se podría modificar la tabla de rutas del host destino. En el caso de sistemas finales, no equipos de red, no es necesario ni el envío ni la recepción de estos paquetes.

Para los dispositivos Cisco, mediante el comando "`no ip redirects`" se evita que los Routers envíen estos paquetes. Por defecto los Routers Cisco no escuchan estas notificaciones.

En el caso de Windows, A través del editor del registro (regedt32.exe) debe localizarse la clave:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
```

Bajo la misma es necesario añadir el valor:

```
Value Name: EnableICMPRedirects
Data Type: REG_DWORD
Value: 0
```

4.2.3.23 SNMP

Como norma general, las redes de gestión deberían implementarse separadas de las redes de servicio (out of band). La primera recomendación concreta se basa en no emplear para los agentes SNMP las claves o nombres por defecto para los permisos de lectura (*RO*) y escritura (*RW*), respectivamente "*public*" y "*private*".

4.2.3.24 OTRAS MEDIDAS

Por otro lado es importante tener en cuenta que no solo es utilizar técnicas basadas en configuraciones y código, también es importante realizar labores de ingeniería social.

La ingeniería social es importante durante la mitigación de los ataques, pues es necesario que todas las personas que conforman la organización, tengan una conciencia de cómo actuar frente a este tema.

Se debe educar a todas las personas de realizar actos de identificación de los ataques, de tal forma que puedan ser de gran ayuda para las personas encargadas, y así poder actuar de forma más rápida y segura.

CAPITULO 5. CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

Las redes de datos hoy en día funcionan bajo un modelo basado en capas de protocolos, denominado modelo OSI, el cual como el TCP/IP se ha convertido en estándar de las comunicaciones actuales. Debido a esto se ha desarrollado mucha literatura enfocada al funcionamiento de dichos modelos, buscando evidenciar sus aspectos más importantes de funcionamiento, entre los cuales se encuentra la seguridad.

Así mismo como se ha realizado estudios sobre la seguridad en dichos modelos, también se han desarrollado nuevas amenazas y vulnerabilidades que se han enfocado estrictamente a atacar los protocolos de cada capa y buscar la manera de hacer el mayor daño posible a las redes de las empresas u organizaciones que no estén preparadas para prevenirlos, detectarlos y mitigarlos.

Este documento entonces se debe considerar como parte de esa literatura resaltando la importancia de la seguridad en el modelo OSI aplicado a una red de datos de una organización. Por eso se aporta como conclusión, que aunque las tecnologías en redes siguen avanzado permitiendo en gran medida controlar el acceso no autorizado de usuarios o personas en una red de una organización, aun muchas de ellas siguen siendo vulnerables a las intrusiones de hackers, sin importar el tipo de ataque que se haga, ya sea por la falta de conocimiento del valor de su información, por el desconocimiento de los mismos ataques o por la falta de políticas de seguridad claras que sean estrictamente impuestas por parte de los administradores de los sistemas de información de tal manera que sirva de blindaje ante posibles modelos de ataques.

Es importante entonces tener en cuenta los aspectos mencionados sobre los tipos de ataques, vulnerabilidades y forma de mitigación, para tener una visión más clara del impacto operacional en los procesos de una organización y así poder dimensionar la verdadera importancia de que la red de datos del sistema de información se encuentre completamente segura.

5.2 RECOMENDACIONES

Este documento tiene como compromiso servir de apoyo a cualquier persona u organización que tenga interés, además de la protección de la información con la cual labora, tener nociones sobre lo que puede afectar cualquier sistema de información y los métodos que se podrían utilizar para prevenir, detectar y responder ante los múltiples ataques que existen en el medio de las redes.
Por tal motivo este documento se ve obligado a presentar sus recomendaciones sobre este caso de estudio.

De acuerdo a la necesidad sobre seguridad en redes se dio origen a un grupo de estándares, los cuales normalizan el comportamiento general que debe cumplir la seguridad en redes, permitiendo un mayor control y mejor funcionamiento de las mismas. Se sugiere que las personas encargadas de los sistemas de información se impregnen de este conocimiento con el fin de contribuir a la preservación de la armonía en los entornos de red.

Con los estándares ya asimilados cualquier administrador de un sistema de información o de redes podría tener la facultad de analizar la infraestructura que posee su organización y así mismo cumplir con los requerimientos mediante políticas de seguridad basadas en dichos estándares. Las políticas de seguridad pueden variar de acuerdo a la infraestructura de red y a las necesidades de la empresa.

Dentro de las políticas de seguridad de una empresa es esencial que además de los administradores, los demás usuarios tenga noción de cuál es el valor de la

información que se maneja, con el fin de asistir en el proceso de protegerla, para lograr esto es necesario que los encargados de las áreas de sistemas y telecomunicaciones estén actualizados sobre los posibles ataques a la red y compartan esta información con las demás áreas de la organización.

Generalmente la administración de una red implica que se conozcan los usuarios que tienen permiso de ingresar al sistema, además de los movimientos que estos hagan dentro. Cabe entonces incluir en las políticas de seguridad que cada usuario sea debidamente registrado para poder controlar el acceso al Sistema

Otras Herramientas muy importantes dentro de la organización son sus antivirus, firewalls, sistemas operativos, entre otros. Lo realmente importante es que estos actúen de la mejor forma, sin embargo la constante evolución de los ataques obliga a que estas herramientas pierdan vigencia con el tiempo, para esto cada organización debe contar con sistemas actualizados, procedimiento que se logra con la adquisición de software legal y licenciado, en cuanto a los sistemas operativos deben contar con parches en su última versión.

Los Backup también deben ser considerados como una obligación dentro de los términos de seguridad de la organización, con esto se previene la perdida y se asegura la integridad de la información.

Se hace necesario que las contraseñas de los equipos y usuarios sea cambiada con frecuencia, recomendable que estas sean de carácter complejo, es decir, que consten de caracteres, letras, números y que no contengan datos personales de los usuarios. Teniendo en cuenta que muchos ataques tienen como objetivo revelarlas.

Dentro de los estándares de seguridad, también abarca la adecuación de las instalaciones físicas sobre las cuales se soporta las topologías de red, se debe tener en cuenta que dentro de esas instalaciones el acceso debe ser limitado a solo personal autorizado.

Puesto que en el futuro de las telecomunicaciones se piensa implementar mecanismos de seguridad mas avanzados utilizando técnicas de inteligencia artificial como las redes neuronales, es importante asociar esos mecanismos a las estrategias que se vayan a implementar en cuanto a la seguridad de las organizaciones, ya que las redes neuronales se fundamentan en el autoaprendizaje.

Es recomendable acelerar la migración de los protocolos IPv4 a IPv6, ya que éste se adecua más estrictamente a las necesidades de seguridad que se está exigiendo por parte de las organizaciones de hoy en día.

Por último, “No se atenga a un solo método de prevención detección y respuesta” la razón se fundamenta en que muchas organizaciones solo apoyan su seguridad sobre herramientas como antivirus y firewalls, desconociendo que existen otra cantidad de métodos para hacer más segura la red, los cuales han sido mencionados en el desarrollo de este documento.

BIBLIOGRAFÍA

[1] ArCERT, Manual de Seguridad en Redes. P.11,17

[2] ARELLANO, Gabriel. Enterprise Security & Risk: Seguridad en Capa 2. p.11,19-23

[3] BARCELÓ ORDINAS, José María; ÍÑIGO GRIERA; MARTÍ ESCALÉ, Ramón; PEIG OLIVÉ, Enric; PERRAMON TORNIL, Xavier. Redes de Computadores. Barcelona: 1 ed, 2004. p.47

[4] BÍSARO, Mauricio y DANIZIO, Eduardo. Curso de Capacitación en Networking. Capítulo 1: Laboratorio de Redes - Diseño y Configuración de Redes de Computadoras. p. 1-7.

[5] BOLT BERANEK y NEWMAN INC ARLINGTON VA, A History of the ARPANET: The First Decade. 1981.

[6] BSI (British Standards Institution 2012). Seguridad de la Información ISO/IEC 27001. [en línea.] <http://www.bsigroup.es/certificacion-y-auditoria/Sistemas-de-gestion/estandares-esquemas/Seguridad-de-la-Informacion-ISOIEC27001/> [Citado el 28 de Febrero de 2012].

[7] CISCO SYSTEMS, CCNA Exploration 1. Capítulo 3: Protocolos y Funcionalidad de la Capa de Aplicación. p.3.1.2

[8] CISCO SYSTEMS, CCNA Exploration 1. Capítulo 4: Capa de Transporte del Modelo OSI. p.4.1.1 – 4.1.5.2

[9] CISCO SYSTEMS. CCNA Exploration 1. Capítulo 7: Capa de Enlace de Datos. p. 7.6.1

[10] CISCO SYSTEMS, CCNA Exploration 1. Capítulo 8: Capa Física del Modelo OSI. p.8.0.1 - 8.3.1

[11] Curso de TCP/IP: ICMP (Protocolo de Mensajes de Control de Internet). p.1-3.

[12] El Modelo OSI y Los Protocolos de Red, Capitulo 2, p.31.

[13]ICONTEC, Presentación de tesis, trabajos de grado y otros trabajos de Investigación, Sexta Actualización, Bogotá 2008.

[14] ISO (INTERNATIONAL ORGANIZATION OF ESTANDARDIZATION). ISO/IEC 27001:2005. [en línea].
<http://www.iso.org/iso/catalogue_detail?csnumber=42103>. [Citado el 28 de Febrero de 2012].

[15] JOLMAN, ALEXANDER. Seguridad Informática. [en línea.] < http://jrobledoherrera.blogspot.com/2009/02/seguridad-informatica.html>. [Citado el 25 de Febrero de 2012].

[16] MARRO, Guillermo Mario. Attacks at the Link Layer. California, 2003. p. 12-14

[17] MIERES, Jorge. Ataques Informáticos: Debilidades de Seguridad Comúnmente Explotadas, 2009. p. 8-15.

[18] MODELO OSI. [en línea]. < http://www.monografias.com/trabajos29/modelo-osi.shtml >. [Citado el 30 de Febrero de 2012].

[19] MONTAÑANA, Profesor. Redes de Comunicaciónes. Madrid: Güimi, 2009. p.4, 6 - 9

[20] PÁEZ , Raúl, Análisis de Seguridad de la Familia de Protocolos TCP/IP y sus Servicios Asociados, 1 ed, 2002. p.23.63-93

[21] TALBOT, David, INFORMÁTICA: Un nuevo software malicioso nos acerca un paso más a la cirberguerra. [en línea]. <http://www.technologyreview.es/read_article.aspx?id=38970 >. [Citado el 8 de Marzo de 2011].

[22] WIKIPEDIA ORG. Address Resolution Protocol. [en línea.] < http://es.wikipedia.org/wiki/Address_Resolution_Protocol>. [Citado el 3 de Marzo de 2012].